
UNIVERSITY OF TORONTO
3 1761 01214792 2

94

537c

LES

FONCTIONS POLYÉDRIQUES

ET MODULAIRES.

PARIS. — IMPRIMERIE GAUTHIER-VILLARS,
44087 Quai des Grands-Augustins, 55.

G. VIVANTI,
PROFESSEUR A LA FACULTÉ DES SCIENCES DE PAVIE.

LES FONCTIONS POLYÉDRIQUES ET MODULAIRES.

OUVRAGE TRADUIT

PAR

Armand CAHEN,
AGRÉGÉ DE L'UNIVERSITÉ, DOCTEUR ÈS SCIENCES,
PROFESSEUR AU LYCÉE D'ÉVREUX.



135.247
23/11/14

PARIS,
GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE
DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.

1910

QA
343
V513

Tous droits de traduction et de reproduction réservés.

PRÉFACE.

Le but que je me propose en écrivant le présent Ouvrage est très modeste : permettre au lecteur d'aborder sans difficultés les leçons classiques de M. Klein sur *l'Icosaèdre* (¹) et de MM. Klein et Fricke sur les *Fonctions modulaires* (²).

Les *Leçons sur l'Icosaèdre* sont un modèle d'élégance géométrique et une véritable mine d'idées nouvelles et géniales, mais la lecture en est assez difficile ; elles renferment une foule de sujets dispersés et à peine esquissés ; et, lors même qu'on a saisi chacune des théories partielles, leurs points communs restent imperceptibles et n'apparaissent qu'après un long travail et un remaniement complet de toute la matière.

Quant à l'Ouvrage sur les *Fonctions modulaires*, ses dimensions considérables et l'extrême variété des sujets qu'il renferme font qu'il ne se prête pas aisément à une première étude.

Tels sont, du moins, les résultats de mon expérience personnelle.

J'ai donc cru bien faire de publier l'œuvre d'élaboration accomplie pour mon usage personnel, facilitant ainsi au lecteur la compréhension de ces théories difficiles et lui épargnant un travail similaire, utile assurément, mais extrêmement pénible.

Était-ce une entreprise trop hardie que d'avoir essayé

(¹) F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*. Leipzig, 1884.

(²) F. Klein und R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen*. Leipzig, 1890-1892.

d'enfermer dans un espace relativement restreint les principes de ces vastes et importantes théories? Peut-être.

Cependant, malgré la grande concision qui m'était imposée, il m'a semblé utile d'associer les deux théories, afin d'éviter des répétitions et de montrer que la théorie de l'Icosaèdre qui, dans le domaine de l'Analyse, pourrait apparaître comme un élégant édifice isolé, et d'un type spécial, n'est autre que la première d'une série de constructions du même genre reliées étroitement entre elles. Il eût sans doute été préférable de faire un pas de plus, en traitant ici même la théorie des fonctions automorphes, mais on comprendra facilement que c'était dépasser les bornes du possible.

Qu'il me soit permis d'adresser l'expression de ma vive et profonde gratitude à mon distingué collègue M. Armand Cahen qui a bien voulu se charger de la traduction française de cet Ouvrage et à M. Gauthier-Villars qui, avec tant d'empressement, en a accepté la publication.

Pavie, avril 1910.

G. Vivanti.



LES

FONCTIONS POLYÉDRIQUES

ET MODULAIRES.

PREMIÈRE PARTIE.

LES GROUPES POLYÉDRIQUES ET LE GROUPE MODULAIRE.

Éléments de la théorie des groupes d'opérations.

1. En Mathématiques, on désigne habituellement sous le nom d'*opération* un acte de l'entendement par lequel on passe d'un ou plusieurs éléments d'une certaine classe à un autre élément de la même classe. Telle est, par exemple, l'addition qui permet, étant donnés plusieurs nombres, d'en déduire un nouveau nombre suivant un mode déterminé.

Nous nous bornerons aux opérations où l'on passe d'*un* élément *unique* d'une certaine classe à *un* autre élément *unique* de la même classe. Telle serait, par exemple, pour les points d'un plan, une rotation d'angle donné autour d'un point fixe du même plan : cette rotation transforme chaque point du plan en un autre point bien déterminé.

De même qu'en Mécanique on considère le repos comme un cas particulier du mouvement (mouvement nul), de même nous regarderons encore comme une opération l'acte qui consiste à remplacer chaque élément par cet élément lui-même. Une telle opération est dite *opération identique* ou *identité;* on la représente souvent par le chiffre 1.

On appelle *opération inverse* d'une opération P une seconde opération supprimant l'effet de la première, en sorte que, si l'opé-

ration P transforme l'élément A en l'élément B, l'opération inverse transforme B en A.

On représente habituellement par P^{-1} l'opération inverse de P.

2. On appelle *produit* de deux opérations P, Q et l'on désigne par la notation PQ ([1]) l'opération donnant lieu aux mêmes effets que les deux opérations P et Q effectuées successivement. On définit de la même manière le produit d'un nombre quelconque d'opérations.

Il est facile de s'assurer sur des exemples (*voir* n° 20) que le produit de plusieurs opérations ne possède pas, en général, la propriété commutative, mais possède au contraire la propriété associative.

Deux opérations P et Q, telles qu'on ait

$$PQ = QP,$$

sont dites *permutables*.

On a évidemment

$$1.P = P.1 = P;$$

par suite, l'opération identique est permutable avec n'importe quelle opération.

La dernière relation écrite justifie bien la notation choisie pour l'opération identique.

Si P et Q sont deux opérations, l'opération $Q^{-1}PQ = P'$ est dite la *transformée de* P *par* Q.

La condition nécessaire et suffisante pour que $P' = P$ *est que* P et Q *soient permutables.*

En effet, si

$$PQ = QP,$$

il en résulte

$$Q^{-1}PQ = Q^{-1}QP = P$$

et inversement, si

$$Q^{-1}PQ = P.$$

On en déduit aussitôt

$$PQ = QP.$$

([1]) Certains auteurs écrivent QP au lieu de PQ. Voici comment une telle notation peut se justifier; soit a un élément : si Pa désigne le résultat de sa transformation par P, QPa désignera le résultat de la transformation de Pa par Q, c'est-à-dire l'élément obtenu en appliquant à a successivement les opérations P et Q.

Avec notre notation, on a au contraire

$$PQa = Q(Pa).$$

Soient P *et* Q *deux opérations quelconques : si*, P *transformant l'élément* a *en l'élément* a', Q *transforme* a *et* a' *en* a_1 *et* a'_1, *l'opération* $Q^{-1}PQ$ change a_1 en a'_1.

En effet, par hypothèse,

$$a' = Pa, \qquad a_1 = Qa, \qquad a'_1 = Qa';$$

d'où il suit

$$a'_1 = Q(Pa) = PQa = PQ(Q^{-1}a_1) = Q^{-1}PQa_1.$$

3. L'opération donnant lieu aux mêmes effets que l'opération P répétée n fois se désigne ordinairement par P^n.

Adoptant, à propos des exposants, les mêmes conventions qu'en Arithmétique, nous représenterons par P^0 l'opération P non effectuée, c'est-à-dire, quel que soit P, l'identité; et nous représenterons par P^{-1} l'opération qui multipliée par P donne l'identité, c'est-à-dire (nº 1) l'opération inverse de P.

Plus généralement, P^{-n} sera l'opération inverse de P^n.

4. On appelle *groupe* un ensemble d'opérations telles que le produit de deux opérations quelconques de l'ensemble appartienne encore au même ensemble. Par exemple, toutes les rotations autour d'un axe donné forment un groupe.

On dit qu'un groupe est *fini* ou *infini*, suivant qu'il se compose d'un nombre fini ou infini d'opérations.

L'*ordre* d'un groupe fini est le nombre d'opérations qu'il comprend.

Un groupe contenu dans un autre groupe est dit *sous-groupe* de ce dernier.

Les opérations permutables avec une même opération forment un groupe.

Soient P, P' deux opérations permutables avec une même opération Q; on aura

$$PQ = QP, \qquad P'Q = QP';$$

d'où, à cause de la propriété associative du produit,

$$(PP')Q = P(P'Q) = P(QP') = (PQ)P' = (QP)P' = Q(PP').$$

Ainsi PP' est bien une opération permutable avec Q.

5. *Les opérations communes à deux groupes constituent un groupe.*

Car, si P et P′ appartiennent à deux groupes, il en est de même de l'opération PP′.

Si, à une opération P donnée, il correspond un entier $t = a$, tel que la relation

$$P^t = 1 \tag{1}$$

soit satisfaite, il en existe évidemment une infinité d'autres : tels seraient, par exemple, tous les multiples de a. Le plus petit des entiers t satisfaisant à la relation (1) est dit l'*ordre* de l'opération P. Ainsi une rotation d'amplitude $\frac{2\pi}{n}$ autour d'un axe est une opération d'ordre n [1].

Soient P *une opération d'ordre* n, Q *une opération quelconque; la transformée de* P *par* Q *est aussi d'ordre* n.

En effet,

$$(Q^{-1}PQ)^n = Q^{-1}PQ\,Q^{-1}PQ\ldots Q^{-1}PQ = Q^{-1}P^nQ = Q^{-1}Q = 1.$$

Soit P *une opération d'ordre* n; *tout nombre* t *satisfaisant à* $P^t = 1$ *est un multiple de* n.

En effet, si t n'était pas multiple de n, la division de t par n donnerait

$$t = qn + r \qquad \text{avec} \qquad n > r > 0,$$

par suite

$$1 = P^t = P^{qn+r} = P^{qn}P^r = (P^n)^qP^r = P^r,$$

ce qui est impossible, puisque $r < n$.

Si P *est une opération d'ordre* n, *son inverse est* P^{n-1}; *elle est aussi d'ordre* n.

En effet, de

$$PP^{n-1} = 1$$

on déduit

$$P^{n-1} = P^{-1}.$$

---

(1) Il existe évidemment des opérations qui ne sont pas d'ordre fini. Par exemple, la multiplication par un nombre entier m différent de $+1$ ou de -1, quel que soit le nombre de fois qu'on la répète, ne donne jamais l'identité.

De plus, $n-1$ et n étant premiers entre eux, le plus petit nombre m pour lequel $P^{(n-1)m}$ est une puissance de P^n est $m=n$.

On trouverait d'une façon analogue

$$P^{n-h}=P^{-h}.$$

Donc, soit P une opération d'ordre n; considérons une de ses puissances; on peut, sans altérer la signification de ce dernier symbole, augmenter ou diminuer l'exposant de la puissance d'un multiple entier quelconque de n.

6. *Les puissances (d'exposant positif, nul ou négatif) d'une même opération forment un groupe.*

En effet,

$$P^r P^s = P^{r+s}.$$

De plus, l'ensemble des puissances positives forme un groupe, et il en est de même pour les puissances négatives.

Les puissances d'une opération d'ordre fini forment un groupe fini, dont l'ordre est égal à celui de l'opération donnée.

Soit P une opération d'ordre n; les puissances

$$P,\quad P^2,\quad P^3,\quad \ldots,\quad P^{n-1},\quad P^n=1$$

sont les seules qui soient distinctes.

En effet, si m est un nombre n'appartenant pas à la suite $1, 2, 3, \ldots, n-1, n$, on peut, en lui ajoutant ou lui retranchant un multiple convenable de n, obtenir un des n premiers nombres entiers, soit r par exemple; alors (n° 5)

$$P^m = P^r.$$

D'autre part, r et s $(r>s)$ étant deux nombres de la suite $1, 2, \ldots, n$, si l'on avait $P^r=P^s$, il en résulterait $P^{r-s}=1$, ce qui est impossible puisque $r-s$ n'est égal ni à zéro, ni à un multiple de n.

Le groupe formé de l'identité et des $n-1$ premières puissances d'une opération d'ordre n est appelé *un groupe cyclique.*

Tout groupe, formé des puissances d'une même opération d'ordre fini, est un groupe cyclique : car, en désignant par P^r la plus petite puissance de P figurant dans le groupe, celui-ci comprendra

exclusivement toutes les puissances de P^r, comme il est facile de s'en assurer.

7. *Si deux puissances d'une opération sont égales entre elles, l'opération est d'ordre fini.*

En effet, si $P^r = P^s$, soit $r > s$, il en résulte

$$P^{r-s} = 1.$$

Les opérations d'un groupe fini sont toutes d'ordre fini.

En effet, soit P une opération du groupe G; toutes les puissances de P appartiennent au même groupe. Mais puisque G ne comprend qu'un nombre fini n d'opérations, parmi les opérations de la suite

$$P, \quad P^2, \quad P^3, \quad \ldots, \quad P^{n+1},$$

deux au moins seront égales. Donc P est une opération d'ordre fini.

8. *Tout groupe fini possède les deux propriétés suivantes :*

a. Il contient l'opération identique;

b. Il contient l'inverse de chacune de ses opérations.

Si P fait partie d'un groupe fini G, elle est d'un ordre fini m (n° 7), par suite

$$P^m = 1.$$

Mais P^m appartient à G, d'où la propriété a.

De plus, P^{m-1} fait partie également de G, et, comme (n° 5) P^{m-1} est l'inverse de P, la propriété b en résulte.

Il n'est pas inutile de faire remarquer que les propriétés a et b n'appartiennent pas toujours aux groupes infinis.

Par exemple (n° 6), le groupe formé des puissances successives d'une opération d'ordre infini ne possède aucune de ces deux propriétés.

9. *L'ordre d'un sous-groupe d'un groupe fini est un diviseur de l'ordre du groupe.*

Soient G un groupe fini d'ordre n, H un de ses sous-groupes d'ordre r, formé des opérations

$$P_0 = 1, \ P_1, \ P_2, \ \ldots, \ P_{r-1}. \tag{1}$$

Si Q_1 est une opération de G n'appartenant pas à la suite (1), les opérations

$$(2) \qquad P_0 Q_1 = Q_1,\ P_1 Q_1,\ P_2 Q_1,\ \ldots,\ P_{r-1} Q_r,$$

qui toutes appartiennent à G, sont distinctes entre elles et différentes des opérations (1).

Car, si l'on avait

$$P_i Q_1 = P_h Q_1,$$

il en résulterait

$$P_i = P_h,$$

et, si l'on avait

$$P_i Q_1 = P_h,$$

il en résulterait

$$P_i^{-1} P_h = Q_1,$$

ce qui est impossible, puisque, P_i^{-1} appartenant à H(nº 8), il en serait de même de $P_i^{-1} P_h$ et par suite de Q_1.

S'il existe dans G d'autres opérations que (1) et (2), et si Q_2 est l'une d'entre elles, on pourra considérer r nouvelles opérations

$$P_0 Q_2 = Q_2,\ P_1 Q_2,\ P_2 Q_2,\ \ldots,\ P_{r-1} Q_2,$$

distinctes l'une de l'autre et différentes des opérations (1) et (2). Et ainsi de suite. Mais, puisque G est un groupe fini, on obtiendra finalement toutes les opérations rangées dans le Tableau suivant, où $s = \frac{n}{r}$ [1] :

$$(\mathrm{T})^{(2)} \quad \left\{ \begin{array}{lllll} P_0 = 1 & P_1 & P_2 & \ldots & P_{r-1} \\ P_0 Q_1 = Q_1 & P_1 Q_1 & P_2 Q_1 & \ldots & P_{r-1} Q_1 \\ P_0 Q_2 = Q_2 & P_1 Q_2 & P_2 Q_2 & \ldots & P_{r-1} Q_2 \\ \ldots\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ P_0 Q_{s-1} = Q_{s-1} & P_1 Q_{s-1} & P_2 Q_{s-1} & \ldots & P_{r-1} Q_{s-1} \end{array} \right.$$

(1) D'où il suit qu'un groupe dont l'ordre est un nombre premier n'admet aucun sous-groupe sauf lui-même et l'unité.

(2) Il est évident qu'au Tableau (T) on peut substituer le suivant :

$$(\mathrm{T}') \quad \left\{ \begin{array}{lllll} P_0 = 1, & P_1, & P_2, & \ldots, & P_{r-1}, \\ Q_1 P_0 = Q_1, & Q_1 P_1, & Q_1 P_2, & \ldots, & Q_1 P_{r-1}, \\ Q_2 P_0 = Q_2, & Q_2 P_1, & Q_2 P_2, & \ldots, & Q_2 P_{r-1}, \\ \ldots\ldots & \ldots & \ldots & \ldots & \ldots \\ Q_{s-1} P_0 = Q_{s-1}, & Q_{s-1} P_1, & Q_{s-1} P_2, & \ldots, & Q_{s-1} P_{r-1}, \end{array} \right.$$

où les Q_i peuvent différer de ceux du Tableau (T). La distribution des opérations de G, correspondant aux différentes lignes, n'est pas, en général, la même dans les deux Tableaux.

La relation $s = \frac{n}{r}$ montre que n est toujours un multiple de r.

Si l'on prend dans chacune des lignes du Tableau (T) une opération quelconque, l'ensemble des opérations ainsi obtenues constitue ce qu'on appelle un *système d'opérations représentantes* du groupe G relativement au sous-groupe H.

Le nombre s de lignes du Tableau (T) est l'*indice* du sous-groupe H dans le groupe G. C'est le rapport des ordres des deux groupes, quand ils sont finis. Un groupe infini peut avoir aussi des sous-groupes d'indice fini ([1]).

10. Soient G un groupe fini d'ordre n, P une de ses substitutions, m l'ordre de P. Le groupe cyclique d'ordre m (n° 6) engendré par P est un sous-groupe de G ; par suite, (n° 9), m est un diviseur de n. Donc *l'ordre d'une substitution appartenant à un groupe fini est un diviseur de l'ordre du groupe.*

11. Étant donnés deux sous-groupes G_1 et G_2 d'un même groupe fini G, respectivement d'indices s_1 et s_2, soient G_3 le groupe des opérations communes (n° 4) à G_1 et G_2, s_3 l'indice de G_3 par rapport à G.

Nous allons démontrer que

$$s_3 \leq s_1 s_2.$$

Posons

$$r_i s_i = n \qquad (i = 1, 2, 3),$$

n étant l'ordre de G.

Soient

$$1, \quad P_1, \quad P_2, \quad \ldots, \quad P_{r_1-1}$$

les opérations de G_1 et, parmi elles,

$$1, \quad P_1, \quad P_2, \quad \ldots, \quad P_{r_3-1}$$

celles qui constituent G_3.

Formons pour le sous-groupe G_1 le Tableau (T) :

1	P_1	P_2	...	P_{r_1-1}
Q_1	$P_1 Q_1$	$P_2 Q_1$	...	$P_{r_1-1} Q_1$
...	.....	.....	...	....
Q_{s_1-1}	$P_1 Q_{s_1-1}$	$P_2 Q_{s_1-1}$,	...	$P_{r_1-1} Q_{s_1-1}$

([1]) *Voir*, par exemple, le n° 93 et les suivants.

Soient Q_1, Q_2, ..., Q_{t_1-1} les Q_i contenus dans G_2 ; on a évidemment $t_1 \leqq s_1$.

Le Tableau

$$\begin{array}{ccccc} 1 & P_1 & P_2 & .. & P_{r_3-1} \\ Q_1 & P_1 Q_1 & P_2 Q_2 & \ldots & P_{r_3-1} Q_1 \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots\ldots \\ Q_{t_1-1} & P_1 Q_{t_1-1} & P_2 Q_{t_1-1} & \ldots & P_{r_3-1} Q_{t_1-1} \end{array}$$

contiendra toutes les opérations de G_2, en sorte que

$$r_3 t_1 = r_2.$$

Il en résulte

$$r_2 \leqq r_3 s_1$$

ou

$$s_3 \leqq s_1 s_2.$$

12. *Si l'on transforme toutes les opérations d'un groupe par une même opération, on obtient un nouveau groupe, dit groupe transformé du premier par cette opération.*

En effet, si P'_1 et P'_2 sont les transformés de P_1 et P_2 par l'opération Q, $P'_1 P'_2$ est la transformée de $P_1 P_2$ par la même opération. En effet, des relations

$$Q^{-1} P_1 Q = P'_1, \qquad Q^{-1} P_2 Q = P'_2$$

on déduit

$$Q^{-1} P_1 P_2 Q = Q^{-1} P_1 Q Q^{-1} P_2 Q = P'_1 P'_2.$$

Il peut arriver que le transformé de G par une opération Q soit identique à G. On dit alors que G est *permutable* avec l'opération Q.

Si le groupe donné est cyclique, il en est de même de son transformé.

En effet, soient P^r la forme générale des opérations du groupe et $Q^{-1} P Q = P'$; on aura

$$Q^{-1} P^r Q = Q^{-1} P Q Q^{-1} P Q \ldots Q^{-1} P Q = P'^r.$$

Supposons que le groupe considéré soit le sous-groupe H d'un certain groupe G et que Q soit une opération de G ; alors le transformé de H par Q, qu'on peut représenter par la relation $Q^{-1} H Q$, est un sous-groupe de G.

Les sous-groupes H et $Q^{-1}HQ$ sont dits *équivalents*. En particulier, si R est une opération du groupe G, les opérations R et $Q^{-1}RQ$ sont dites *équivalentes*.

Quand le groupe considéré comprend l'identité et l'inverse de chacune de ses opérations, l'équivalence possède les trois propriétés fondamentales de l'égalité.

En effet :

1° *Chaque sous-groupe est équivalent à lui-même.*

Car

$$1^{-1}H1 = H.$$

2° *Si* H *est équivalent à* H', H' *est équivalent à* H.

Car si l'on a

$$Q^{-1}HQ = H',$$

il en résulte

$$H = QH'Q^{-1} = (Q^{-1})^{-1}H'(Q^{-1}),$$

relation qui exprime l'équivalence de H' et de H, puisque Q^{-1} est une opération du groupe.

3° *Si* H *est équivalent à* H' *et que* H' *soit équivalent à* H'', H *est équivalent à* H''.

En effet, de

$$Q^{-1}HQ = H', \qquad Q'^{-1}H'Q' = H''$$

on déduit

$$Q'^{-1}Q^{-1}HQQ' = H'',$$

ou bien

$$(QQ')^{-1}H(QQ') = H'',$$

qui exprime l'équivalence de H et de H'', QQ' étant une opération de groupe.

Il peut arriver que les deux groupes H et $Q^{-1}HQ$ soient identiques : en particulier, cela arrivera nécessairement si Q est une opération de H, H possédant les propriétés *a* et *b* énoncées au numéro 8. Si, Q étant une opération de G, les deux sous-groupes H et $Q^{-1}HQ$ sont identiques, on dit que H est un sous-groupe *invariant* de G.

13. *Si* H *est un sous-groupe non invariant de* G, *on peut toujours déterminer un sous-groupe* K *de* G, *contenant* H et *admettant* H *comme sous-groupe invariant.*

Observons tout d'abord que l'ensemble des opérations de G, possédant la propriété de transformer H en lui-même, constitue un groupe K. En effet, de

$$Q_1^{-1} H Q_1 = H, \qquad Q_2^{-1} H Q_2 = H$$

on déduit

$$Q_2^{-1} Q_1^{-1} H Q_1 Q_2 = H,$$

c'est-à-dire

$$(Q_1 Q_2)^{-1} H (Q_1 Q_2) = H.$$

Le groupe K ainsi défini contient H, puisque, ainsi qu'on vient de le voir, chaque opération de K transforme H en lui-même; de plus, H est évidemment un sous-groupe invariant de K.

On peut encore remarquer que K est le plus grand sous-groupe de G admettant H comme sous-groupe invariant.

Soient

$$1, \quad Q_1, \quad Q_2, \quad \ldots, \quad Q_{r-1}$$

les opérations de K; construisons le Tableau (T) relatif à ce sous-groupe, et soit $rs = n$, n étant l'ordre de G :

$$\begin{array}{lllll} 1 & Q_1 & Q_2 & \ldots & Q_{r-1} \\ R_1 & Q_1 R_1 & Q_2 R_1 & \ldots & Q_{r-1} R_1 \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots\ldots \\ R_{s-1} & Q_1 R_{s-1} & Q_2 R_{s-1} & \ldots & Q_{r-1} R_{s-1} \end{array}$$

Il est facile de voir que les opérations d'une même ligne de ce Tableau transforment H en un sous-groupe équivalent.

En effet, puisque

$$Q_h^{-1} H Q_h = H \qquad (h = 1, 2, \ldots, r-1),$$

il vient

$$(Q_h R_i)^{-1} H (Q_h R_i) = R_i^{-1} Q_h^{-1} H Q_h R_i = R_i^{-1} H R_i \qquad (i = 1, 2, \ldots, s-1),$$

résultat indépendant de h. Donc :

Les différents sous-groupes équivalents à H, *y compris* H *lui-même, sont en nombre s, c'est-à-dire en nombre égal à l'indice de* K.

Ce nombre est par suite un diviseur de n.

Le sous-groupe formé des opérations communes à tous les sous-groupes équivalents entre eux est un sous-groupe invariant, car il n'est équivalent qu'à lui-même.

14. Soient

$$G_m = (1, P_1, P_2, \ldots, P_{m-1}), \qquad G_n = (1, Q_1, Q_2, \ldots, Q_{n-1})$$

deux groupes finis d'opérations, tels que toutes les opérations du premier soient permutables avec celles du second. Les opérations

$$(1) \quad \begin{cases} 1 & P_1 & P_2 & \ldots & P_{m-1} \\ Q_1 & Q_1 P_1 & Q_1 P_2 & \ldots & Q_1 P_{m-1} \\ Q_2 & Q_2 P_1 & Q_2 P_2 & \ldots & Q_2 P_{m-1} \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots\ldots \\ Q_{n-1} & Q_{n-1} P_1 & Q_{n-1} P_2 & \ldots & Q_{n-1} P_{m-1} \end{cases}$$

constituent un groupe G_{mn}, dont G_m et G_n sont deux sous-groupes invariants.

En effet, on a tout d'abord

$$Q_i P_h Q_k P_l = Q_i Q_k P_h P_l = Q_r P_s.$$

Ensuite

$$(Q_i P_h)^{-1} P_t (Q_i P_h) = P_h^{-1} Q_i^{-1} P_t Q_i P_h = P_h^{-1} P_t P_h = P_u,$$
$$(Q_i P_h)^{-1} Q_t (Q_i P_h) = P_h^{-1} Q_i^{-1} Q_t Q_i P_h = Q_i^{-1} Q_t Q_i = Q_r.$$

Examinons comment, des sous-groupes de G_m et de G_n, on pourra déduire ceux de G_{mn}.

Soient

$$G_\mu = (1, P_1, P_2, \ldots, P_{\mu-1}), \qquad G_\nu = (1, Q_1, Q_2, \ldots, Q_{\nu-1})$$

deux sous-groupes, l'un de G_m, l'autre de G_n. Les opérations

$$(2) \quad \begin{cases} 1 & P_1 & P_2 & \ldots & P_{\mu-1} \\ Q_1 & Q_1 P_1 & Q_1 P_2 & \ldots & Q_1 P_{\mu-1} \\ Q_2 & Q_2 P_1 & Q_2 P_2 & \ldots & Q_2 P_{\mu-1} \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots\ldots \\ Q_{\nu-1} & Q_{\nu-1} P_1 & Q_{\nu-1} P_2 & \ldots & Q_{\nu-1} P_{\mu-1} \end{cases}$$

constituent un sous-groupe $G_{\mu\nu}$ de G_{mn}, qu'on pourra considérer comme le résultat de la *combinaison* des sous-groupes G_μ et G_ν. Mais, réciproquement, tout sous-groupe de G_{mn} ne provient pas nécessairement de la combinaison de deux sous-groupes appartenant à G_m et G_n. Soient G_ρ un sous-groupe de G_{mn}, et G_μ, G_ν les plus grands sous-groupes qui lui soient communs respectivement avec G_m et G_n; le groupe G_ρ contiendra évidemment $G_{\mu\nu}$. Si $\rho = \mu\nu$

les deux groupes G_ρ et $G_{\mu\nu}$ sont identiques. Si au contraire $\rho > \mu\nu$, G_ρ contiendra, en même temps que les opérations du Tableau (2), d'autres opérations. Soit $Q_i P_h$ une opération de G_ρ; il contiendra aussi les opérations

$$Q_i P_h P_1, \quad Q_i P_h P_2, \quad \ldots, \quad Q_i P_h P_{\mu-1}.$$

Mais $P_h P_1$, $P_h P_2$, ..., $P_h P_{\mu-1}$ sont $\mu - 1$ opérations de G_m, que nous désignerons par P_{h_1}, P_{h_2}, ..., $P_{h_{\mu-1}}$; en sorte que, si G_ρ contient $Q_i P_h$, il contient en outre les $\mu - 1$ opérations

$$Q_i P_{h_j} \qquad (j = 1, 2, \ldots, \mu - 1).$$

Il ne peut en contenir d'autres, dans lesquelles i aurait la même valeur; car soit $Q_i P_k$ une telle opération, où k est distinct de tous les h_j; en posant

$$P_k = P_h P_l,$$

on aurait nécessairement $l > \mu - 1$ et G_ρ devrait contenir aussi l'opération

$$(Q_i P_h)^{-1} Q_i P_h P_l = P_l,$$

tandis que, par hypothèse,

$$1, \quad P_1, \quad P_2, \quad \ldots, \quad P_{\mu-1}$$

sont les seules opérations qu'il comprenne.

Il résulte de là que, si G_ρ contient une opération d'une ligne du Tableau (1), il en contient μ appartenant à la même ligne. La considération des colonnes du Tableau (1) donne lieu à des conclusions analogues.

Si $\rho > \mu\nu$, G_ρ contient, outre les éléments (1), d'autres éléments qui, moyennant des changements convenables d'indices, peuvent être rangés comme il suit :

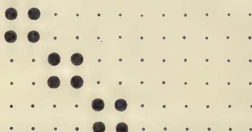
$$(3) \quad \left\{ \begin{array}{cccc} Q_\nu P_\mu & Q_\nu P_{\mu+1} & \ldots & Q_\nu P_{2\mu-1} \\ Q_{\nu+1} P_\mu & Q_{\nu+1} P_{\mu+1} & \ldots & Q_{\nu+1} P_{2\mu-1} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ Q_{2\nu-1} P_\mu & Q_{2\nu-1} P_{\mu+1} & \ldots & Q_{2\nu-1} P_{2\mu-1} \end{array} \right.$$

et ainsi de suite. Les rectangles (2), (3), etc. sont contenus dans le rectangle (1) et sont tous groupés autour d'une même oblique, qu'ils admettent pour diagonale, comme on le voit sur la

figure, où l'on suppose

$$m = 12, \qquad n = 6, \qquad \mu = \nu = 2, \qquad \rho = 12 = 3 \times 4.$$

On a représenté par des points les éléments de G_{mn}, et indiqué d'une façon plus apparente ceux d'entre eux qui appartiennent à G_ρ :



Posons $\rho = \theta\mu\nu$. Nous pouvons choisir comme opérations représentantes de G_ρ relativement à $G_{\mu\nu}$ les opérations

$$1, \quad Q_\nu P_\mu, \quad Q_{2\nu} P_{2\mu}, \quad \ldots, \quad Q_{(\theta-1)\nu} P_{(\theta-1)\mu}.$$

Les opérations

$$1, \quad P_1, \quad P_2, \quad \ldots, \quad P_{(\theta-1)\mu}$$

forment un sous-groupe $G_{\mu\nu}$ de G_m. Montrons qu'elles forment effectivement un groupe. En effet, si $Q_i P_h$, $Q_k P_l$ sont deux opérations de G_ρ avec les conditions $h \leqq \theta\mu - 1$, $l \leqq \theta\mu - 1$,

$$Q_i P_h Q_k P_l = Q_i Q_k P_h P_l = Q_r P_s$$

appartient à G_ρ, s étant $\leqq \theta\mu - 1$. Donc le produit de deux opérations

$$P_j \qquad (j \leqq \theta\mu - 1)$$

est une opération du même ensemble.

De même les opérations

$$1, \quad Q_1, \quad Q_2, \quad \ldots, \quad Q_{(\theta-1)\nu}$$

forment un sous-groupe $G_{\theta\nu}$ de G_n.

En combinant $G_{\mu\nu}$ et $G_{\theta\nu}$, sous-groupes de G_m et G_n, on obtient un sous-groupe

$$G_{\theta^2\mu\nu} = G_{\theta\rho}$$

de G_{mn}, contenant G_ρ comme sous-groupe [1]; c'est évidemment le plus petit sous-groupe *combiné* ayant une telle propriété.

Donc, si G_ρ est un sous-groupe ne provenant pas d'une combinaison, on peut construire deux sous-groupes combinés, l'un G_μ contenu dans G_ρ, l'autre $G_{\theta^2\mu\nu}$ qui renferme G_ρ. Si l'on désigne les sous-groupes non combinés sous le nom de *sous-groupes intermédiaires*, on peut dire que *les sous-groupes de* G_{mn} *sont* ou *combinés*, ou *intermédiaires*.

On peut observer que G_μ est un sous-groupe invariant de $G_{\theta\mu}$. En effet, si P_i appartient à G_μ et P_k à $G_{\theta\mu}$, il existe dans G_ρ une opération $Q_h P_k$, donc aussi l'opération

$$(Q_h P_k)^{-1} P_i Q_h P_k = P_k^{-1} P_i P_k = P_l.$$

Mais G_ρ est le plus grand sous-groupe commun à G_ρ et à G_m; donc P_l, qui appartient à chacun d'eux, fait partie de G_μ. De même G_ν est un sous-groupe invariant de $G_{\theta\nu}$; on en déduit immédiatement que $G_{\mu\nu}$ est un sous-groupe invariant de $G_{\theta^2\mu\nu}$ et par suite de G_ρ.

Observons encore que, comme représentantes de $G_{\theta\mu}$ par rapport à G_μ et de $G_{\theta\nu}$ par rapport à G_ν, on peut prendre respectivement les opérations

$$1,\quad P_\mu,\quad P_{2\mu},\quad \ldots,\quad P_{(\theta-1)\mu};\qquad 1,\quad Q_\nu,\quad Q_{2\nu},\quad \ldots,\quad Q_{(\theta-1)\nu}.$$

D'après cela, étant donnés deux groupes G_m, G_n et deux de leurs sous-groupes respectifs G_μ, G_ν, cherchons à construire deux sous-groupes $G_{\mu'}$, $G_{\nu'}$ de G_m, G_n, admettant respectivement G_μ et G_ν comme sous-groupes invariants, et dont les ordres soient proportionnels à μ et ν.

Posons $\mu' = \theta\mu$, $\nu' = \theta\nu$ et choisissons un système de représentantes de $G_{\theta\mu}$ relativement à G_μ, soit $1, P_\mu, P_{2\mu}, \ldots, P_{(\theta-1)\mu}$, et un système de représentantes de $G_{\theta\nu}$, soit $1, Q_\nu, Q_{2\nu}, \ldots, Q_{(\theta-1)\nu}$. Avec ces éléments nous pourrons construire un sous-groupe intermédiaire de G_{mn}. Il est clair que si, laissant fixe par exemple l'ordre des premières représentantes, nous faisons varier celui des

---

[1] Il serait représenté sur la figure par un carré de dimensions 6 dont un sommet coïncide avec le sommet supérieur de gauche du rectangle principal.

secondes, nous obtiendrons en général des sous-groupes intermédiaires différents.

15. Tout groupe contient au moins deux sous-groupes invariants : le groupe lui-même et le groupe formé de la seule substitution identique. Si un groupe ne contient pas d'autres sous-groupes invariants que les deux précédents, il est dit *simple;* dans le cas contraire, le groupe est dit *composé.*

Tout groupe fini dont l'ordre est un nombre premier est un groupe simple (*voir* n° 9).

Un groupe est dit *transitif* relativement à une classe déterminée de quantités, si, étant données deux quantités quelconques de cette classe, il existe toujours dans le groupe une opération permettant de passer de l'une quelconque de ces deux quantités à l'autre. Dans le cas contraire, le groupe est dit *intransitif.*

16. Soient deux groupes G et G′ ; si l'on peut établir entre eux une correspondance telle qu'à chaque opération de G corresponde dans G′ une opération, et une seule, et que, au produit de deux opérations de G, corresponde le produit des deux opérations correspondantes de G′, on dit que les deux groupes sont *isomorphes.* L'isomorphisme est dit *holoédrique* quand, à des opérations différentes de G, correspondent toujours des opérations différentes de G′ ; il est dit *mériédrique* dans le cas contraire.

Deux groupes holoédriquement isomorphes sont identiques entre eux au point de vue formel et ne peuvent différer que par la nature des opérations qui les constituent. Si les deux groupes sont finis, ils ont le même ordre.

Soient G et G′ deux groupes isomorphes; je dis qu'à l'identité dans G correspond l'identité dans G′. Supposons, en effet, qu'à l'opération 1 de G corresponde dans G′ une opération Q différente de 1 ; alors, P et P′ étant deux opérations correspondantes de G et G′, à $1 . P = P$ dans G correspondrait dans G′ l'opération QP′, qui est différente de P′. Maintenant, si l'isomorphisme est mériédrique, il y aura plusieurs opérations de G correspondant dans G′ à l'identité. De telles opérations forment un groupe, car, si à P et Q correspond dans G′ l'opération 1, cette même opération correspondra

encore dans G' à l'opération PQ de G. De plus ce groupe, que nous représentons par G_0, est un sous-groupe invariant de G [1]. En effet, si P est une opération de G_0 et Q' l'opération de G' correspondant à P, à l'opération $Q^{-1}PQ$ de G correspondra dans G' l'opération

$$Q^{-1}\,1\,Q' = 1,$$

en sorte que $Q^{-1}PQ$ appartient aussi à G_0.

Il est ensuite facile de voir que, si à l'opération R de G correspond l'opération R' de G', on obtient l'ensemble des opérations de G correspondant à R' en multipliant par R les opérations de G_0. D'où il suit que l'ordre de G_0 est le quotient des ordres de G et G'. Ce quotient est appelé *degré de mériédrie*. Dans le cas particulier où ce quotient est égal à 2, l'isomorphisme est dit *hémiédrique*.

Substitutions linéaires.

17. Appliquons les généralités précédentes à une classe importante d'opérations : les substitutions linéaires.

On appelle *substitution linéaire* l'opération permettant de passer d'une valeur quelconque à une autre z', liée à z par une relation de la forme

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}, \tag{1}$$

α, β, γ, δ étant des quantités réelles ou complexes, assujetties à l'unique condition

$$\alpha\delta - \beta\gamma \neq 0. \tag{2}$$

La substitution (1) se représente quelquefois par la notation abrégée

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

La quantité $\alpha\delta - \beta\gamma$ s'appelle le *déterminant* de la substitution.

Observons que, quel que soit c, pourvu qu'il ne soit pas nul, on

[1] Il suit de là que, si G est un groupe simple, l'isomorphisme ne saurait être hémiédrique.

a toujours

$$(3) \qquad \begin{pmatrix} c\alpha & c\beta \\ c\gamma & c\delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix};$$

d'où il résulte, en tenant compte de (2), qu'on peut toujours, sans altérer le sens d'une substitution, l'amener à une forme telle qu'on ait

$$(4) \qquad \alpha\delta - \beta\gamma = 1.$$

Nous appellerons substitution *unitaire* toute substitution linéaire dont le déterminant est égal à 1 ; et, sauf avertissement contraire, nous ne considérons dans la suite que des substitutions linéaires de cette espèce.

Résolvant (1) par rapport à z,

$$(5) \qquad z = \frac{\delta z' - \beta}{-\gamma z' + \alpha},$$

puis échangeant z' et z, on obtient

$$z' = \frac{\delta z - \beta}{-\gamma z + \alpha}$$

qui est l'opération inverse de (1). Donc :

L'opération inverse d'une substitution linéaire est une substitution linéaire.

Pour

$$\alpha = \delta = 1, \qquad \beta = \gamma = 0,$$

(1) devient $z' = z$, c'est-à-dire la substitution identique.

Les formules (1) et (5) montrent qu'une substitution linéaire fait correspondre à toute valeur de z une valeur de z' et une seule et réciproquement à toute valeur de z' une valeur unique de z.

Si l'on se reporte à la représentation géométrique connue des nombres complexes, on peut considérer une substitution linéaire comme une transformation biunivoque des points d'un plan en ceux d'un autre plan, ou encore, quand z et z' sont deux points d'un même plan, comme une transformation biunivoque d'un plan en lui-même.

On sait que, dans une telle transformation, les angles sont con-

servés; il en est de même, d'ailleurs, pour toutes celles de la forme

$$z' = f(z),$$

$f(z)$ étant une fonction analytique de la variable complexe z au sens de Cauchy-Riemann.

18. Étant donnée une substitution linéaire non identique

$$(1) \qquad z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$

on peut se demander s'il existe des valeurs de z égales aux valeurs z' qui leur correspondent.

En faisant dans (1) $z' = z$, on obtient

$$(2) \qquad \gamma z^2 + (\delta - \alpha) z - \beta = 0.$$

Cette équation admet deux racines distinctes ou non, sauf dans le cas de la substitution identique ($\alpha = \delta = 1$, $\beta = \gamma = 0$); nous avons exclu ce cas exceptionnel, où (2) se réduit à une identité.

Donc : *Une substitution linéaire non identique laisse invariables une ou deux valeurs de* z. On donne à ces valeurs de z le nom de *pôles* de la substitution.

19. Examinons maintenant quelques types particuliers de substitutions :

$$(a) \qquad z' = z + h.$$

Tous les points du plan subissent un déplacement mesuré par un vecteur égal à h; d'où le nom de *translation* donné à la substitution correspondante. Toute figure est transformée en une figure égale. La substitution a un seul pôle, qui est le point à l'infini du plan [1] :

$$(b) \qquad z' = kz.$$

Posons

$$z = \rho e^{i\varphi}, \qquad z' = \rho' e^{i\varphi'}, \qquad k = c e^{i\alpha};$$

d'où

$$\rho' = c\rho, \qquad \varphi' = \varphi + \alpha.$$

---

[1] On sait que, dans la théorie des fonctions de variables complexes, on considère le plan comme ayant un seul point à l'infini.

On voit que le rayon vecteur de chaque point se trouve multiplié par un facteur constant, tandis que son argument est augmenté d'une quantité constante. C'est donc une transformation par similitude ayant pour centre l'origine, suivie d'une rotation autour du même point; nous désignerons cette substitution sous le nom de *torsion*. Les deux pôles sont ici l'origine et le point à l'infini.

Indiquons comme cas particuliers de la torsion : la *rotation* et l'*extension*, correspondant respectivement aux hypothèses $c = 1$, $\alpha = 0$.

(*c*)
$$z' = -\frac{1}{z}.$$

Posons
$$z = x + iy, \qquad z' = x' + iy';$$
d'où
$$x' = -\frac{x}{x^2 + y^2}, \qquad y' = \frac{y}{x^2 + y^2}, \qquad x'^2 + y'^2 = \frac{1}{x^2 + y^2}.$$

La dernière relation écrite laisse inaltéré le cercle de rayon *un* ayant pour centre l'origine et change la région intérieure à ce cercle en la région extérieure et réciproquement. D'où le nom d'*inversion* donné à cette substitution. Les deux pôles sont ici les points $+i$ et $-i$.

L'équation
$$a(x^2 + y^2) + 2(bx + cy) + d = 0$$
représente en général un cercle. Ce cercle se réduit à une droite si $a = 0$.

En lui appliquant la substitution précédente, on obtient
$$d(x'^2 + y'^2) + 2(-bx' + cy') + a = 0,$$
équation d'un cercle, qui, pour $d = 0$, se réduit à une droite.

Donc, en considérant la ligne droite comme un cas particulier du cercle, on peut dire que *l'inversion transforme un cercle en un autre cercle*.

Il est évident que cette dernière propriété appartient également aux deux autres types de substitutions considérés.

20. Soient deux substitutions linéaires
$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad S' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix};$$

S change z en

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$

et S′ change z' en

$$z'' = \frac{\alpha' z' + \beta'}{\gamma' z' + \delta'} = \frac{(\alpha'\alpha + \beta'\gamma)z + (\alpha'\beta + \beta'\delta)}{(\gamma'\alpha + \delta'\gamma)z + (\gamma'\beta + \delta'\delta)},$$

de sorte que la substitution SS′ change z en

$$\frac{(\alpha'\alpha + \beta'\gamma)z + (\alpha'\beta + \beta'\delta)}{(\gamma'\alpha + \delta'\gamma)z + (\gamma'\beta + \delta'\delta)};$$

on voit donc que *le produit de deux substitutions linéaires est une substitution linéaire,* donnée par la formule suivante :

(1) $$SS' = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha'\alpha + \beta'\gamma & \alpha'\beta + \beta'\delta \\ \gamma'\alpha + \delta'\gamma & \gamma'\beta + \delta'\delta \end{pmatrix}.$$

Si l'on échange S et S′ on aura

$$S'S = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}.$$

On voit qu'en général SS′ et S′S sont deux opérations différentes.

21. *Toute substitution linéaire peut être mise sous la forme d'un produit de translations, de torsions et d'inversions.*

En effet, en tenant compte des relations (3) et (4) du numéro 17, on vérifie facilement que

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \gamma & \delta \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \gamma^2 \end{pmatrix} \begin{pmatrix} \gamma & \alpha \\ 0 & \gamma \end{pmatrix}.$$

Des quatre substitutions qui figurent dans le second membre, la première et la dernière sont des translations, la deuxième est une inversion et la troisième une torsion. D'où il suit (n° 19), la ligne droite étant toujours considérée comme un cas particulier du cercle, que :

Toute substitution linéaire change un cercle en un autre cercle.

22. *Étant donnés deux triangles ayant leurs côtés formés de segments de droites ou d'arcs de cercle et leurs angles respectivement égaux, il existe une substitution linéaire, les transformant l'un dans l'autre* ([1]).

Soient les triangles ABC, $A_1B_1C_1$, dont les angles de même nom sont égaux. Supposons d'abord les côtés AB et AC rectilignes. Une translation T amènera le point A au point A_1, puis une rotation R fera coïncider les côtés AB et A_1B_1, et, à cause de l'égalité des angles, le côté AC coïncidera avec le côté A_1C_1.

Dans cette nouvelle position les figures ABC, $A_1B_1C_1$ seront homothétiques, et, au moyen d'une extension H, on pourra changer ABC en $A_1B_1C_1$. Donc, dans le cas considéré, ABC se transformera en $A_1B_1C_1$ par la substitution linéaire TRH.

Supposons maintenant que AB et AC ne soient pas tous deux rectilignes; appelons D le second point d'intersection des deux cercles ou du cercle de la droite, auxquels AB et AC appartiennent. Toute substitution S, pour laquelle D devient le point à l'infini, changera ABC en un triangle $A'B'C'$ ayant les côtés $A'B'$ et $A'C'$ rectilignes.

Soit S_1 la substitution analogue à S, transformant $A_1B_1C_1$ en $A'_1B'_1C'_1$. Alors, moyennant une substitution TRH, $A'B'C'$ se transformera en $A'_1B'_1C'_1$, et l'on pourra passer de ABC à $A_1B_1C_1$ par la substitution

$$STRHS_1^{-1}.$$

23. Soit $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une substitution linéaire ayant deux pôles distincts p et q. Ils ont pour expression

$$\left.\begin{matrix} p \\ q \end{matrix}\right\} = \frac{\alpha-\delta\pm\sqrt{(\alpha-\delta)^2+4\beta\gamma}}{2\gamma} = \frac{\alpha-\delta\pm\sqrt{(\alpha+\delta)^2-4}}{2\gamma}.$$

Comme p et q satisfont à l'équation (2) (n° 18), on aura

$$\gamma p^2+(\delta-\alpha)p-\beta=0,$$
$$\gamma q^2+(\delta-\alpha)q-\beta=0;$$

d'où successivement

$$-p(\alpha-\gamma p)=\beta-\delta p,$$
$$-q(\alpha-\gamma q)=\beta-\delta q;$$

([1]) Le lecteur est prié de faire la figure.

et

$$z' - p = \frac{\alpha z + \beta}{\gamma z + \delta} - p = \frac{(\alpha - \gamma p)z + \beta - \delta p}{\gamma z + \delta} = \frac{(\alpha - \gamma p)(z - p)}{\gamma z + \delta},$$

$$z' - q = \frac{\alpha z + \beta}{\gamma z + \delta} - q = \frac{(\alpha - \gamma q)z + \beta - \delta q}{\gamma z + \delta} = \frac{(\alpha - \gamma q)(z - q)}{\gamma z + q}$$

et enfin

(1) $$\frac{z' - p}{z' - q} = \theta \frac{z - p}{z - q}.$$

Calculons la valeur de θ :

$$\theta = \frac{\alpha - \gamma p}{\alpha - \gamma q} = \frac{(\alpha - \gamma p)^2}{(\alpha - \gamma p)(\alpha - \gamma q)} = \frac{(\alpha - \gamma p)^2}{\alpha^2 - \alpha\gamma(p + q) + \gamma^2 pq}.$$

Mais

$$p + q = \frac{\alpha - \delta}{\gamma}, \qquad pq = -\frac{\beta}{\gamma}.$$

Par suite

$$\alpha^2 - \alpha\gamma(p + q) + \gamma^2 pq = \alpha\delta - \beta\gamma = 1,$$

d'où

$$\theta = (\alpha - \gamma p)^2 = \left(\frac{\alpha + \delta - \sqrt{(\alpha + \delta)^2 - 4}}{2}\right)^2 \quad [1].$$

Cette expression de θ montre que le genre d'une substitution unitaire dépend uniquement de la somme de ses coefficients extrêmes.

La substitution (1) a reçu des dénominations diverses, suivant la valeur de θ.

Si $|\theta| = 1$, on dit que la substitution est *elliptique;* si θ est réel et positif, la substitution est *hyperbolique;* dans tous les autres cas, elle est *loxodromique.*

24. *Si $\alpha + \delta$ est réel, la substitution ne peut être loxodromique.*

Soit d'abord

$$|\alpha + \delta| > 2;$$

alors θ est réel et la substitution est hyperbolique.

---

[1] Si $\gamma = 0$, un des pôles, q par exemple, est à l'infini et la substitution prend la forme plus simple

$$z' - p = \theta(z - p) \qquad \text{avec} \qquad \theta = \alpha^2.$$

Soit au contraire

$$|\alpha+\delta|<2 \quad (^1).$$

Posons

$$\alpha+\delta=2k \qquad (|k|<1);$$

on a

$$\theta=(k-i\sqrt{1-k^2})^2.$$

Mais

$$|k-i\sqrt{1-k^2}|=\sqrt{k^2+(1-k^2)}=1;$$

alors $|\theta|=1$ et la substitution est elliptique.

Une substitution loxodromique est le produit d'une substitution elliptique et d'une substitution hyperbolique.

En effet, si $\theta=ce^{i\alpha}$, la substitution

$$\frac{z'-p}{z'-q}=\theta\frac{z-p}{z-q}$$

est le produit des deux substitutions suivantes, prises dans un ordre quelconque,

$$\frac{z'-p}{z'-q}=e^{i\alpha}\frac{z-p}{z-q}, \qquad \frac{z'-p}{z'-q}=c\frac{z-p}{z-q},$$

dont la première est elliptique, et la seconde hyperbolique.

25. Soit maintenant $\begin{pmatrix}\alpha & \beta\\ \delta & \gamma\end{pmatrix}$ une substitution linéaire dont les deux pôles coïncident. La condition pour qu'il en soit ainsi est

$$\alpha+\delta=\pm 2.$$

L'unique pôle r est

$$r=\frac{\alpha-\delta}{2\gamma}$$

avec

$$\alpha-\gamma r=\gamma r+\delta.$$

On a de plus (nº 23)

$$-r(\alpha-\gamma r)=\beta-\delta r,$$

d'où

$$z'-r=\frac{\alpha z+\beta}{\gamma z+\delta}-r=\frac{(\alpha-\gamma r)z+\beta-\delta r}{\gamma z+\delta}=\frac{(\alpha-\gamma r)(z-r)}{\gamma z+\delta}$$
$$=\frac{(\alpha-\gamma r)(z-r)}{\gamma(z-r)+\gamma r+\delta}=\frac{(\alpha-\gamma r)(z-r)}{\gamma(z-r)+\alpha-\gamma r},$$

(¹) Si $\alpha+\delta$ est réel, on ne peut avoir $|\alpha+\delta|=2$, car il en résulterait $(\alpha+\delta)^2=4$ et les deux pôles ne seraient pas distincts.

qu'on peut écrire

$$\frac{1}{z'-r} = \eta + \frac{1}{z-r},$$

η ayant pour valeur

$$\eta = \frac{\gamma}{\alpha - \gamma r} = \frac{2\gamma}{\alpha + \gamma} = \pm \gamma.$$

Les substitutions à pôle unique sont dites *paraboliques*.

26. *La transformée d'une substitution par une autre est de même espèce que la substitution primitive.*

Soient

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

deux substitutions quelconques. Comme (n° 17)

$$Q^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

on a (n° 20)

$$Q^{-1}P = \begin{pmatrix} \alpha d - \beta c & -\alpha b + \beta a \\ \gamma d - \delta c & -\gamma b + \delta a \end{pmatrix}$$

et, par suite,

$$Q^{-1}PQ = \begin{pmatrix} \alpha ad - \beta ac + \gamma bd - \delta bc & -\alpha ab + \beta a^2 - \gamma b^2 + \delta ab \\ \alpha cd - \beta c^2 + \gamma d^2 - \delta cd & -\alpha bc + \beta ac - \gamma bd + \delta ad \end{pmatrix},$$

en sorte que, si l'on pose

$$Q^{-1}PQ = P' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix},$$

on aura

$$(1) \quad \left\{ \begin{aligned} \alpha' &= \alpha ad - \beta ac + \gamma bd - \delta bc, \\ \beta' &= -\alpha ab + \beta a^2 - \gamma b^2 + \delta ab, \\ \gamma' &= \alpha cd - \beta c^2 + \gamma d^2 - \delta cd, \\ \delta' &= -\alpha bc + \beta ac - \gamma bd + \delta ad. \end{aligned} \right.$$

En tenant compte de $ad - bc = 1$, on obtient

$$\alpha' + \delta' = \alpha + \delta,$$

relation qui établit le théorème.

27. La signification géométrique des substitutions linéaires

apparaîtra plus clairement, si l'on fait un changement de variables.

Considérons d'abord la substitution, avec deux pôles,

$$(1) \qquad \frac{z'-p}{z'-q} = \theta \frac{z-p}{z-q}$$

et substituons à z la nouvelle variable Z liée à z par

$$Z = \frac{z-p}{z-q}.$$

La relation (1) devient

$$(2) \qquad Z' = \theta Z.$$

Considérons la torsion

$$(3) \qquad Z' = \theta^{\lambda} Z,$$

où l'exposant λ peut varier d'une façon continue par valeurs positives et croissantes de la valeur 0, correspondant à la substitution identique, à la valeur 1, correspondant à la substitution (2).

Si la substitution est elliptique, (3) représente une rotation. Posons

$$Z = \rho e^{i\varphi}, \qquad Z' = \varphi' e^{i\varphi'}, \qquad \theta = e^{i\alpha};$$

il vient

$$\rho' = \rho, \qquad \varphi' = \varphi + \lambda\alpha,$$

qui représente une torsion, de sorte que le point mobile, en passant de la position initiale à la position finale, décrit autour de l'origine un arc de cercle d'amplitude α.

Si la substitution est hyperbolique, (3) représente une extension. Posons

$$\theta = c, \qquad \text{d'où} \qquad \rho' = c^{\lambda}\rho, \qquad \varphi' = \varphi,$$

et le point mobile parcourt un segment de droite appartenant à un rayon issu de l'origine.

Enfin, si la substitution est loxodromique, posons $\theta = ce^{i\alpha}$; alors

$$\rho' = c^{\lambda}\rho, \qquad \varphi' = \varphi + \lambda\alpha.$$

Le rayon vecteur et l'argument varient, l'un suivant une progression géométrique, l'autre suivant une progression arithmétique, et, par suite, le point mobile décrit une spirale logarithmique dont le pôle est à l'origine.

Nous désignerons en général sous le nom de *trajectoire* de la substitution les lignes parcourues par le point mobile dans ces différents cas.

28. Imaginons une sphère tangente au plan Z à l'origine, et projetons stéréographiquement le plan sur cette sphère, en choisissant pour pôle de transformation le point de la sphère diamétralement opposé au point de contact. Si l'on prend comme axe le diamètre passant par ces deux derniers points, les droites du plan issues de l'origine et les cercles du plan ayant l'origine pour centre se projettent respectivement sur la sphère suivant des méridiens et des parallèles.

Considérons maintenant des spirales logarithmiques, ayant leur pôle à l'origine. On sait qu'elles coupent sous un angle constant les droites issues du même point. Comme la transformation stéréographique conserve les angles, ces spirales se projettent sur la sphère suivant des courbes appelées *loxodromies* et rencontrant les méridiens sous un angle constant; de là le nom de *substitution loxodromique*.

29. Revenons maintenant au plan z, en nous bornant aux substitutions elliptiques et hyperboliques; on passe du plan z au plan Z par la substitution linéaire

$$Z = \frac{z-p}{z-q}.$$

Aux cercles de l'un des plans correspondent des cercles de l'autre plan; et aux points p et q du plan z correspondent les points o et ∞ du plan Z. Donc, dans le plan Z le faisceau des rayons issus de l'origine, rayons qui peuvent être considérés comme des cercles passant par les points o et ∞, aura pour transformé dans le plan z la famille des cercles passant par p et q.

Quant aux substitutions elliptiques, pour obtenir leurs trajectoires, il suffit d'observer que, à cause de $|\theta| = 1$, on a

$$\left|\frac{z'-p}{z'-q}\right| = \left|\frac{z-p}{z-q}\right|,$$

relation qui exprime que le rapport des distances du point mobile

aux deux points p et q est constant. Les trajectoires sont donc des cercles, admettant p et q pour points conjugués.

Il convient de s'arrêter un instant au cas des substitutions elliptiques, pour mieux déterminer le mouvement du point z'.

Si l'on pose $\theta = e^{i\alpha}$ et si l'on désigne par arg. u l'argument de la quantité complexe u, on a

$$\arg.\frac{z'-p}{z'-q} = \alpha + \arg.\frac{z-p}{z-q}$$

ou bien

$$\arg.(z'-p) - \arg.(z'-q) = \alpha + \arg.(z-p) - \arg.(z-q).$$

Si maintenant P, Q, Z, Z' sont les points du plan représentatif des quantités p, q, z, z',

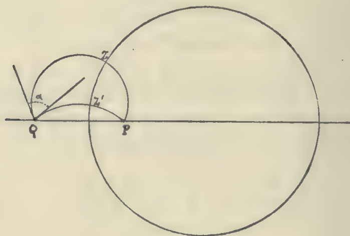
$$\arg.(z-p) - \arg.(z-q) = \text{QZP},$$
$$\arg.(z'-p) - \arg.(z'-q) = \text{QZ'P},$$

en sorte que

$$\text{QZ'P} = \alpha + \text{QZP}.$$

Donc, le point Z étant donné, pour en déduire le point Z', il suffit de construire sur la corde PQ un arc de cercle faisant en P et Q un angle α avec l'arc de cercle PZQ. Le point Z' sera à l'in-

Fig. 1.



tersection de cet arc de cercle et du cercle passant par Z et admettant P et φ pour points conjugués.

30. Passons maintenant aux substitutions à un seul pôle

$$\frac{1}{z'-r} = \gamma_1 + \frac{1}{z-r}.$$

Moyennant le changement de variables

$$Z = \frac{1}{z-r},$$

la substitution devient

$$Z' = \gamma_1 + Z.$$

C'est une translation.

Considérons la substitution

$$Z' = \lambda\gamma_1 + Z,$$

où λ varie par valeurs positives et croissantes de 0 à 1. Le point mobile, pour passer de la position initiale à la position finale, parcourra un segment de grandeur et de direction constantes. Les trajectoires de la substitution sont donc formées d'un faisceau de droites parallèles. Mais on peut envisager deux droites parallèles comme deux cercles dont les points communs sont confondus et rejetés à l'infini. Donc, au faisceau des droites parallèles du plan Z correspondra dans le plan z un faisceau de cercles passant par le point r et tangents en ce point à un droite fixe.

31. *Soient* P *une substitution à pôles distincts p et q*

$$\frac{z'-p}{z'-q} = \theta\,\frac{z-p}{z-q}$$

et $Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *une autre substitution quelconque. L'expression de la substitution* $Q^{-1}PQ$ *est*

$$\frac{z'-p'}{z'-q'} = \theta\,\frac{z-p'}{z-q'},$$

p' et q' ayant pour valeurs

$$p' = \frac{\alpha p + \beta}{\gamma p + \delta}, \qquad q' = \frac{\alpha q + \beta}{\gamma q + \delta}.$$

En effet, pour former la substitution $Q^{-1}PQ$, nous devons éli-

miner z' et z'' entre les équations

$$z = \frac{\alpha z' + \beta}{\gamma z' + \delta}, \qquad \frac{z'' - p}{z'' - q} = \theta \frac{z' - p}{z' - q}, \qquad z''' = \frac{\alpha z'' + \beta}{\gamma z'' + \delta},$$

on obtient ainsi

$$\frac{\dfrac{\delta z''' - \beta}{-\gamma z''' + \alpha} - p}{\dfrac{\delta z''' - \beta}{-\gamma z''' + \alpha} - q} = \theta \frac{\dfrac{\delta z - \beta}{-\gamma z + \alpha} - p}{\dfrac{\delta z - \beta}{-\gamma z + \alpha} - q}$$

ou bien

$$\frac{z''' - \dfrac{\alpha p + \beta}{\gamma p + \delta}}{z''' - \dfrac{\alpha q + \beta}{\gamma q + \delta}} = \theta \frac{z - \dfrac{\alpha p + \beta}{\gamma p + \delta}}{z - \dfrac{\alpha q + \beta}{\gamma q + \delta}}.$$

32. *Soit* P *une substitution à pôle unique* r

$$\frac{1}{z' - r} = \eta + \frac{1}{z - r}$$

et $Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *une autre substitution quelconque, l'expression de la substitution* $Q^{-1}PQ$ est

$$\frac{1}{z' - r'} = \eta' + \frac{1}{z' - r'},$$

r' *et* η' *ayant pour valeurs*

$$r' = \frac{\alpha r + \beta}{\gamma r + \delta}, \qquad \eta' = \eta(\gamma r + \delta)^2.$$

En effet, éliminant z' et z'' entre les équations

$$z = \frac{\alpha z' + \beta}{\gamma z' + \delta}, \quad \frac{1}{z'' - r} = \eta + \frac{1}{z' - r}, \qquad z''' = \frac{\alpha z'' + \beta}{\gamma z'' + \delta},$$

on obtient

$$\frac{1}{\dfrac{\delta z''' - \beta}{-\gamma z''' + \alpha} - r} = \eta + \frac{1}{\dfrac{\delta z - \beta}{-\gamma z + \alpha} - r}$$

ou

$$\frac{1}{\gamma r + \delta} \frac{-\gamma z''' + \alpha}{z''' - \dfrac{\alpha r + \beta}{\gamma r + \delta}} = \eta + \frac{1}{\gamma r + \delta} \frac{-\gamma z + \alpha}{z - \dfrac{\alpha r + \beta}{\gamma r + \delta}},$$

ou encore (en tenant compte de $\alpha\delta - \beta\gamma = 1$)

$$\frac{1}{\gamma r + \delta}\left[-\gamma + \frac{1}{(\gamma r + \delta)\left(z''' - \frac{\alpha r + \beta}{\gamma r + \delta}\right)}\right]$$

$$= r_1 + \frac{1}{\gamma r + \delta}\left[-\gamma + \frac{1}{(\gamma r + \delta)\left(z - \frac{\alpha r + \beta}{\gamma r + \delta}\right)}\right]$$

et enfin

$$\frac{1}{z''' - \frac{\alpha r + \beta}{\gamma r + \delta}} = r_1(\gamma z + \delta)^2 + \frac{1}{z - \frac{\alpha r + \beta}{\gamma r + \delta}}.$$

33. Recherchons maintenant si une substitution linéaire peut être une opération d'ordre fini.

Tout d'abord, la chose est impossible pour une substitution parabolique. En effet, une telle opération équivaut à une translation et, quel que soit le nombre de fois qu'on la répète, elle ne ramène jamais le point mobile à sa position primitive.

Considérons donc les substitutions à deux pôles.

En répétant m fois la substitution

$$(1) \qquad \frac{z' - p}{z' - q} = \theta \frac{z - p}{z - q},$$

on obtient la substitution

$$\frac{z' - p}{z' - q} = \theta^m \frac{z - p}{z - q};$$

pour qu'elle se réduise à l'unité, on doit avoir $\theta^m = 1$. Donc : *Pour qu'une substitution* (1) *à deux pôles soit d'ordre fini, il faut et il suffit que* θ *soit une racine de l'unité, d'indice fini.*

Par suite, *les seules substitutions linéaires d'ordre fini sont les substitutions elliptiques.*

34. *Si deux substitutions d'ordre fini ont les mêmes pôles, on peut en trouver une troisième, dont les deux premières soient des puissances.*

Soient les deux substitutions

$$\frac{z' - p}{z' - q} = \theta \frac{z - p}{z - q}, \qquad \frac{z' - p}{z' - q} = \theta' \frac{z - p}{z - q},$$

d'ordres m et m', n le plus petit commun multiple de m et m', et η' une racine primitive $n^{\text{ième}}$ de l'unité. On aura

$$\theta = \eta^{\frac{hn}{m}}, \qquad \theta' = \eta^{\frac{h'n}{m'}},$$

h et h' étant des nombres entiers. Les deux substitutions données seront alors les puissances d'exposants $\frac{hn}{m}$ et $\frac{h'n}{m'}$ d'une même substitution

$$\frac{z'-p}{z'-q} = \eta\,\frac{z-p}{z-q}.$$

35. Soit G un groupe fini de substitutions ; supposons que $r-1$ d'entre elles $P_1, P_2, \ldots, P_{r-1}$ aient un pôle commun q. En adjoignant à ces dernières substitutions l'identité par rapport à laquelle tous les points peuvent être considérés comme pôles, on forme évidemment un sous-groupe du groupe donné. Car, si P_i et P_h laissent le point q invariable, cela est encore vrai de $P_i P_h$.

Supposons pour simplifier que q soit le point à l'infini ; les P_i prendront la forme (n° 23)

$$z'-p_i = \theta_i(z-p_i) \qquad (i = 1, 2, \ldots, r-1).$$

On trouve facilement pour la substitution $P_i P_h$

$$z' = \theta_i\theta_h z + \sigma,$$

et pour $P_h P_i$

$$z' = \theta_i\theta_h z + \tau,$$

σ et τ ayant pour expressions

$$\sigma = -\theta_h\theta_i p_i + \theta_h(p_i - p_h) + p_h,$$
$$\tau = -\theta_h\theta_i p_h + \theta_i(p_h - p_i) + p_i.$$

De là pour la substitution $(P_h P_i)^{-1}$ ou $P_i^{-1} P_h^{-1}$

$$z' = \frac{z-1}{\theta_i\theta_h},$$

et ensuite pour la substitution $P_i P_h P_i^{-1} P_h^{-1}$

$$z' = \frac{(\theta_i\theta_h z + \sigma) - \tau}{\theta_i\theta_h} = z + \frac{\sigma - \tau}{\theta_i\theta_h} = z - \frac{1}{\theta_i\theta_h}(\theta_i - 1)(\theta_h - 1)(p_i - p_h).$$

Si dans le dernier terme aucun facteur n'était nul, la substi-

tution $P_i P_h P_i^{-1} P_h^{-1}$ serait parabolique; mais cela est impossible, puisque (n° 33) elle appartient à un groupe fini. Et comme $\theta_i \neq 1$, $\theta_h \neq 1$, on doit avoir $p_i = p_h$. Donc les substitutions $P_1, P_2, \ldots, P_{r-1}$ ont les deux pôles communs et sont par conséquent (n° 34) les puissances d'une même substitution. D'où il suit (n° 6) que le groupe $1, P_1, P_2, \ldots, P_{r-1}$ est un groupe cyclique; on arrive donc à la conclusion suivante :

Les substitutions linéaires d'un groupe fini, qui ont en commun un même pôle, ont aussi en commun l'autre pôle et forment un sous-groupe cyclique.

Il résulte aussi du théorème énoncé au n° 31 que :

Si p et q sont les pôles des substitutions d'un sous-groupe cyclique Γ *appartenant à un groupe fini* G, soit $Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une substitution de G; *les substitutions du sous-groupe cyclique* (n° 12) $\Gamma' = Q^{-1}\Gamma Q$ *ont pour pôles*

$$p' = \frac{\alpha p + \beta}{\gamma p + \delta} = Q(p), \qquad q' = \frac{\alpha q + \beta}{\gamma q + \delta} = Q(q).$$

On dit que les pôles p, p' sont *équivalents;* et il en est de même de q, q'.

36. Soient G un groupe fini d'ordre n, Γ le sous-groupe cyclique formé (n° 35) de toutes les substitutions de G ayant les mêmes pôles p et q. Soient $1, P, P^2, \ldots, P^{\nu-1}$ les substitutions de Γ. Formons (n° 9) le Tableau (T) relatif à ce sous-groupe :

$$\begin{array}{lllll}
1, & P, & P^2, & \ldots, & P^{\nu-1}, \\
Q_1, & PQ_1, & P^2Q_1, & \ldots, & P^{\nu-1}Q_1, \\
\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots\ldots, \\
Q_{\frac{n}{\nu}-1}, & PQ_{\frac{n}{\nu}-1}, & P^2Q_{\frac{n}{\nu}-1}, & \ldots, & P^{\nu-1}Q_{\frac{n}{\nu}-1}.
\end{array}$$

Puisque p n'est un pôle que pour les substitutions de la première ligne, les points

$$p_i = Q_i(p) \qquad \left(i = 1, 2, \ldots, \frac{n}{\nu} - 1\right)$$

seront tous différents de p. Ils seront aussi distincts entre eux,

car, si l'on avait

$$Q_i(p) = Q_h(p),$$

il en résulterait

$$p = Q_h Q_i^{-1}(p).$$

Or, les seules substitutions laissant p invariable étant P et ses puissances, on devrait avoir, pour une valeur convenable de l,

$$Q_h Q_i^{-1} = P^l,$$

ou bien

$$Q_h = P^l Q_i,$$

ce qui est impossible, puisque tous les éléments du Tableau sont distincts.

Nous avons donc $\frac{n}{\nu}$ pôles équivalents $p, p_1, p_2, \ldots, p_{\frac{n}{\nu}-1}$, tous distincts, et nous pouvons conclure que :

Le nombre des pôles distincts, équivalents à un pôle donné, y compris ce pôle, est égal à l'indice du sous-groupe formé par les substitutions admettant le pôle donné.

Il est facile de voir que : *Toute substitution du groupe* G *a pour effet d'échanger entre eux les pôles*

$$p, \quad p_1, \quad p_2, \quad \ldots, \quad p_{\frac{n}{\nu}-1}.$$

En effet, soit $P^h Q_k$ l'une d'elles; appliquons cette substitution à un quelconque p_i des pôles considérés.

Nous aurons

$$P^h Q_k(p_i) = Q_i P^h Q_k(p).$$

Mais $Q_i P^h Q_k$, étant un produit de substitutions appartenant à G, est une certaine substitution $P^r Q_s$ de G. Donc

$$P^h Q_k(p_i) = P^r Q_s(p) = p_s.$$

Il est important d'observer que les points $p, p_1, p_2, \ldots$ sont les pôles des sous-groupes Γ, $Q_1^{-1}\Gamma Q_1$, $Q_2^{-1}\Gamma Q_2, \ldots$.

On a vu que les points $p, p_1, p_2, \ldots$ diffèrent tous entre eux; il n'en faut pas déduire qu'il en soit de même pour les sous-groupes correspondants. Au contraire, ces sous-groupes coïncident deux à deux, quand un des points $p, p_1, p_2, \ldots$ se confond avec le second pôle q de Γ. En effet, si $p_i = q$, les substitutions des deux sous-

groupes Γ et $Q_i^{-1}\Gamma Q_i$ ayant un pôle commun ont aussi en commun l'autre pôle (n° 35) et par suite les deux sous-groupes sont identiques. Le même fait se produit pour les autres sous-groupes pris deux à deux, car, si l'on a

$$q = p_i = Q_i(p), \qquad q_h = Q_h(p),$$

il en résulte

$$q_h = Q_i\,Q_h(p) = P^l\,Q_k(p) = p_k.$$

37. Les considérations précédentes permettent de déterminer tous les groupes finis possibles de substitutions linéaires.

Soit G un groupe fini d'ordre n. Les pôles de ses substitutions (autres que l'identité), comptés chacun autant de fois qu'il y a de substitutions auxquelles il appartient, sont en nombre $2n - 2$.

Supposons qu'un pôle soit commun à ν_1 substitutions, l'identité comprise; alors (n° 35) il fait partie d'un système de $\frac{n}{\nu_1}$ pôles équivalents. En raisonnant d'une façon analogue pour les autres pôles, on obtiendra des systèmes de $\frac{n}{\nu_2}, \frac{n}{\nu_3}, \ldots, \frac{n}{\nu_r}$ pôles équivalents. Et comme un pôle du système i appartient à $\nu_i - 1$ substitutions autres que l'identité, on aura

$$\sum_{i=1}^{r} \frac{n}{\nu_i}(\nu_i - 1) = 2n - 2,$$

ou bien encore

$$(1) \qquad \sum_{i=1}^{r} \left(1 - \frac{1}{\nu_i}\right) = 2 - \frac{2}{n}.$$

Nous sommes donc amenés à chercher les systèmes de nombres entiers positifs $\nu_1, \nu_2, \ldots, \nu_k$ et n satisfaisant à cette équation.

On a évidemment

$$n \geqq \nu_i \geqq 2 \qquad (i = 1, 2, \ldots, r),$$

d'où

$$r > \sum_{i=1}^{r} \left(1 - \frac{1}{\nu_i}\right) \geqq \frac{r}{2},$$

$$2 > 2 - \frac{2}{n} \geqq 1.$$

Par suite, en tenant compte de (1),

$$r > 1 \quad \text{et} \quad 2 > \frac{r}{2},$$

ou bien

$$1 < r < 4.$$

Ainsi r ne prendra que les valeurs 2 et 3.

Soit $r = 2$; la relation (1) devient

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} = \frac{2}{n},$$

et, à cause de $\nu_1 \leqq n$, $\nu_2 \leqq n$, elle admet comme unique solution

$$\nu_1 = \nu_2 = n.$$

Soit maintenant $r = 3$; l'équation (1) devient

$$(2) \qquad \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} = 1 + \frac{2}{n}.$$

Si tous les ν_i étaient supérieurs ou égaux à 3, le premier membre serait inférieur ou égal à 1, ce qui est impossible; donc l'un au moins des ν_i est égal à 2.

Soit, par exemple, $\nu_1 = 2$, d'où

$$\frac{1}{\nu_2} + \frac{1}{\nu_3} = \frac{1}{2} + \frac{2}{n}.$$

On ne peut avoir en même temps $\nu_2 \geqq 4$, $\nu_3 \geqq 4$, car alors, le premier membre ne dépasserait pas $\frac{1}{2}$. Donc l'un des ν_2, ν_3 doit avoir la valeur 2 ou la valeur 3.

Supposons d'abord $\nu_2 = 2$; il en résulte $\nu_3 = \frac{n}{2}$, ce qui ne peut avoir lieu que si n est un nombre pair.

Supposons, au contraire, que ni ν_1 ni ν_2 n'ait la valeur 2; l'une d'elles aura la valeur 3. Soit $\nu_2 = 3$. Il en résulte

$$\frac{1}{\nu_3} = \frac{1}{6} + \frac{2}{n},$$

donc $\nu_3 < 6$. Les hypothèses successives $\nu_3 = 3, 4, 6$ conduisent à $n = 12, 24, 60$.

Nous réunissons dans le Tableau suivant toutes les solutions de

l'équation (1), auxquelles correspondent autant de groupes *possibles* de solutions linéaires :

	r.	ν_1.	ν_2.	ν_3.	n.
I.	2	n	n	»	n
II	3	2	2	n	$2m$
III	3	2	3	3	12
IV	3	2	3	4	24
V	3	2	3	5	60

Nous établirons plus loin (n° 35) l'existence effective de tous ces groupes.

38. Les substitutions linéaires et fractionnaires d'une variable peuvent être mises sous forme de substitutions linéaires entières et homogènes de deux variables.

Soit la substitution

$$(1) \qquad z' = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Posons

$$z = \frac{z_1}{z_2}, \qquad z' = \frac{z'_1}{z'_2};$$

il vient

$$\frac{z'_1}{z'_2} = \frac{\alpha z_1 + \beta z_2}{\gamma z_1 + \delta z_2},$$

d'où, λ désignant un facteur quelconque,

$$(2) \qquad z'_1 = \lambda(\alpha z_1 + \beta z_2), \qquad z'_2 = \lambda(\gamma z_1 + \delta z_2).$$

Donc, à toute substitution (1) non homogène correspondent une infinité de substitutions (2) homogènes. Mais, si nous nous bornons aux *substitutions homogènes unitaires*, c'est-à-dire à celles dont le déterminant des coefficients est égal à *un*, à chaque substitution (1) correspondront deux systèmes de substitutions (2).

En effet, le coefficient λ sera déterminé par

$$\lambda^2(\alpha\delta - \beta\gamma) = 1,$$

d'où pour λ les deux valeurs

$$\lambda = \pm \frac{1}{\sqrt{\alpha\delta - \beta\gamma}}.$$

Dans le cas particulier où la substitution (1) est unitaire, les deux valeurs de λ sont $+1$ et -1.

Soit un groupe G de substitutions non homogènes; les substitutions homogènes qui leur correspondent forment évidemment un groupe G′. G′ est hémiédriquement isomorphe à G, et, si G est d'ordre fini, G′ est d'un ordre double. De plus, à l'identité dans G correspondent dans G′ les deux substitutions

$$z'_1 = z_1, \qquad z'_2 = z_2,$$
$$z'_1 = -z_1, \qquad z'_2 = -z_2.$$

Pseudosubstitutions linéaires.

39. Nous appellerons *pseudosubstitution linéaire* [1] l'opération par laquelle on passe d'une valeur quelconque de z à une autre,

$$(1) \qquad z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} + \delta} \qquad (\alpha\delta - \beta\gamma \neq 0),$$

$\bar{z}$ représentant le nombre complexe conjugué de z.

La quantité $\alpha\delta - \beta\gamma$ est dite le *déterminant* de la pseudosubstitution.

Il n'existe aucune pseudosubstitution pouvant se réduire à l'opération identique.

En effet, pour que (1) laisse invariable les valeurs $0, 1, \infty$, il faut qu'on ait successivement $\beta = 0$, $\gamma = 0$, $\alpha = \delta$; (1) se réduit alors à

$$z' = \bar{z}.$$

Mais ce n'est pas là une opération identique : il existe en effet une infinité de valeurs qu'elle ne laisse pas invariables, car elle change chaque valeur conplexe en sa conjuguée.

L'inverse d'une pseudosubstitution est une pseudosubstitution.

---

[1] Pour les pseudosubstitutions, nous sous-entendrons souvent le mot *linéaire* comme nous le faisons pour les substitutions.

En effet, résolvons (1) par rapport à $\bar{z}$

$$\bar{z} = \frac{\delta z' - \beta}{-\gamma z' + \alpha},$$

prenons les conjugués des deux membres et échangeons ensuite z' et z; il vient

$$z' = \frac{\bar{\delta}\bar{z} - \bar{\beta}}{-\bar{\gamma}\bar{z} + \bar{\alpha}}.$$

Le produit de deux pseudosubstitutions est une substitution.

Soient

$$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} + \delta}, \qquad z'' = \frac{\alpha'\bar{z'} + \beta'}{\gamma'\bar{z'} + \delta'}.$$

On tire de la première

$$\bar{z'} = \frac{\bar{\alpha} z + \bar{\beta}}{\bar{\gamma} z + \bar{\delta}}.$$

Transportant cette valeur de $\bar{z'}$ dans la seconde :

$$z'' = \frac{(\alpha'\bar{\alpha} + \beta'\bar{\gamma})z + \alpha'\bar{\beta} + \beta'\bar{\delta}}{(\gamma'\bar{\alpha} + \delta'\bar{\gamma})z + \gamma'\bar{\beta} + \delta'\bar{\delta}}.$$

Le produit d'une pseudosubstitution et d'une substitution, ou bien d'une substitution et d'une pseudosubstitution, est une pseudosubstitution.

En effet, le produit de

$$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} + \delta}, \qquad z'' = \frac{\alpha' z' + \beta'}{\gamma' z' + \delta'}$$

est la pseudosubstitution

$$z'' = \frac{(\alpha'\alpha + \beta'\gamma)\bar{z} + \alpha'\beta + \beta'\delta}{(\gamma'\alpha + \delta'\gamma)\bar{z} + \gamma'\beta + \delta'\delta}.$$

De même, on a, pour le produit de

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}, \qquad z'' = \frac{\alpha'\bar{z'} + \beta'}{\gamma'\bar{z'} + \delta'},$$

la pseudosubstitution

$$z'' = \frac{(\alpha'\bar{\alpha} + \beta'\bar{\gamma})\bar{z} + \alpha'\bar{\beta} + \beta'\bar{\delta}}{(\gamma'\bar{\alpha} + \delta'\bar{\gamma})\bar{z} + \gamma'\bar{\beta} + \delta'\bar{\delta}}.$$

Toute pseudosubstitution est le produit de la pseudosubstitution $z' = -\bar{z}$ et d'une substitution.

On vérifie en effet immédiatement que (1) est le produit de $z' = -z$ et de la substitution $\begin{pmatrix} \alpha & -\beta \\ \gamma & -\delta \end{pmatrix}$.

La pseudosubstitution $z' = -\bar{z}$, qui échange entre eux les points symétriques par rapport à l'axe imaginaire, peut être désigné, sous le nom de *réflexion* sur cet axe.

40. Si l'on regarde une pseudosubstitution Q

$$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} + \delta} \tag{1}$$

comme une transformation en lui-même du plan de la variable complexe, on peut se demander s'il existe des points du plan que cette transformation laisse invariables.

Tout d'abord, il est évident que, si un point n'est pas déplacé par la pseudosubstitution Q, il ne le sera pas non plus par la substitution Q^2. Donc, sauf le cas où Q^2 se réduirait à la substitution identique, Q laissera invariables deux points tout au plus.

Considérons d'abord le cas de $Q^2 = 1$; Q est alors une opération du deuxième ordre, et l'on a (n° 39)

$$Q^2 = \begin{pmatrix} \alpha\bar{\alpha} + \beta\bar{\gamma} & \alpha\bar{\beta} + \beta\bar{\delta} \\ \gamma\bar{\alpha} + \delta\bar{\gamma} & \gamma\bar{\beta} + \delta\bar{\delta} \end{pmatrix}$$

et, à cause de l'hypothèse $Q^2 = 1$,

$$\left\{ \begin{aligned} &\alpha\bar{\alpha} + \beta\bar{\gamma} = \gamma\bar{\beta} + \delta\bar{\delta}, \\ &\alpha\bar{\beta} + \beta\bar{\delta} = 0, \\ &\gamma\bar{\alpha} + \delta\bar{\gamma} = 0. \end{aligned} \right. \tag{2}$$

Si $\beta = \gamma = 0$, la première des relations (2) donne

$$|\alpha| = |\delta|,$$

en sorte que Q devient

$$z' = e^{i\lambda}\bar{z}$$

ou encore

$$z' = \frac{\alpha\bar{z}}{-\bar{\alpha}}$$

en posant

$$\alpha = e^{i\frac{\lambda-\pi}{2}}.$$

Si β et γ ne sont pas nuls en même temps, soit $\gamma \neq 0$. Alors on peut supposer qu'on ait multiplié les quatre coefficients de Q par une quantité telle que γ devienne réel. Dans ces conditions, les relations (2) deviendront

$$\alpha\bar{\alpha} + \beta\gamma = \gamma\bar{\beta} + \delta\bar{\delta}, \qquad \alpha\bar{\beta} + \beta\bar{\delta} = 0, \qquad \gamma(\bar{\alpha} + \delta) = 0;$$

la dernière donne

$$\bar{\alpha} + \delta = 0,$$

c'est-à-dire

$$\delta = -\bar{\alpha},$$

d'où

$$|\alpha| = |\delta|,$$

et alors la première devient

$$\gamma(\beta - \bar{\beta}) = 0,$$

d'où

$$\beta = \bar{\beta}.$$

Quant à la seconde, elle est alors identiquement satisfaite.

Si l'on observe que la condition $\delta = -\bar{\alpha}$ subsiste aussi pour $\beta = \gamma = 0$, on peut en conclure que :

La forme générale des pseudosubstitutions du second ordre est

(3) $$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} - \bar{\alpha}},$$

dans laquelle β *et* γ *sont réels.*

Pour trouver les points que (3) laisse invariables il suffit de poser dans (3) $z' = z$, d'où

(4) $$\gamma z\bar{z} - \bar{\alpha}z - \alpha\bar{z} - \beta = 0,$$

équation d'un cercle [1] de centre $\frac{\alpha}{\gamma}$ et de rayon

$$\rho = \frac{\sqrt{\alpha\bar{\alpha} + \beta\gamma}}{\gamma} = \frac{\sqrt{-\Delta}}{\gamma},$$

où Δ, qui est toujours réel, désigne le déterminant de la pseudosubstitution.

Ce cercle est réel ou imaginaire suivant que $\Delta \gtrless 0$. Pour $\gamma = 0$, il se réduit à une droite. Donc :

La pseudosubstitution du second ordre (3) *ne laisse invariable aucun point du plan, ou bien laisse invariables tous les points d'un cercle, selon que son déterminant est positif ou négatif.*

Le cercle (4) est appelé *cercle de symétrie* de la pseudosubstitution.

41. Cherchons quelle position occupent, par rapport à ce cercle, deux points homologues z et z'; soit d'abord $\gamma = 0$, le cercle de symétrie se réduit à la droite

$$\alpha\bar{z} + \bar{\alpha}z + \beta = 0,$$

et, si ζ est un point de cette droite, on a

$$\alpha\bar{\zeta} + \bar{\alpha}\zeta + \beta = 0. \tag{1}$$

La pseudosubstitution s'écrit, dans le cas actuel,

$$z' = \frac{\alpha\bar{z} + \beta}{-\bar{\alpha}},$$

d'où, quel que soit ζ,

$$-\bar{\alpha}(z' - \zeta) = \alpha\bar{z} + \beta + \bar{\alpha}\zeta$$

---

(1) En effet, si dans (4) on pose

$$z = x + iy, \qquad \alpha = \alpha_1 + i\alpha_2,$$

nous aurons

$$\gamma(x^2 + y^2) - 2\alpha_1 x - 2\alpha_2 y - \beta = 0$$

ou bien

$$\left(x - \frac{\alpha_1}{\gamma}\right)^2 + \left(y - \frac{\alpha^2}{\gamma}\right)^2 = \frac{\alpha_1^2 + \alpha_2^2 + \beta\gamma}{\gamma^2}.$$

et, en particulier, si ζ appartient à la droite de symétrie, en tenant compte de (1),

$$-\bar{\alpha}(z' - \zeta) = \alpha(\bar{z} - \bar{\zeta}),$$

d'où

$$|z' - \zeta| = |\bar{z} - \bar{\zeta}| = |z - \zeta|.$$

La droite de symétrie est, par conséquent, le lieu des points équidistants de z' et de z, c'est-à-dire que *les points* z, z' *sont symétriques par rapport à la droite de symétrie.*

Soit maintenant $\gamma \neq 0$. Puisque

$$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} - \bar{\alpha}},$$

on a, quel que soit ζ,

$$z' - \zeta = \frac{\alpha\bar{z} + \beta - \gamma\bar{z}\zeta + \bar{\alpha}\zeta}{\gamma\bar{z} - \bar{\alpha}}.$$

Or l'équation du cercle de symétrie, cercle de centre $\frac{\alpha}{\gamma}$, peut s'écrire

$$\left|z - \frac{\alpha}{\gamma}\right| = \text{const.},$$

et, si ζ désigne un de ses points, on aura

$$\gamma\zeta\bar{\zeta} - \alpha\bar{\zeta} - \bar{\alpha}\zeta - \beta = 0,$$

$$|\gamma\zeta - \alpha| = \text{const.};$$

d'où

$$z' - \zeta = \frac{\alpha\bar{z} - \gamma\bar{z}\zeta + \gamma\zeta\bar{\zeta} - \alpha\bar{\zeta}}{\gamma\bar{z} - \bar{\alpha}}$$

ou

$$z' - \zeta = -\frac{\gamma\zeta - \alpha}{\gamma\bar{z} - \bar{\alpha}}(\bar{z} - \bar{\zeta}).$$

En égalant les modules des deux membres et tenant compte de la relation $|\gamma\zeta - \alpha| = \text{const.}$, on voit que le rapport $\frac{|z' - \zeta|}{|\bar{z} - \bar{\zeta}|}$, ou bien $\frac{|z' - \zeta|}{|z - \zeta|}$, est indépendant de ζ, pourvu que ζ appartienne au cercle de symétrie; d'où il résulte que *les points* z *et* z' *sont conjugués par rapport au cercle de symétrie.*

Observons que ce résultat comprend comme cas particulier le résultat trouvé pour $\gamma = 0$. On peut donc énoncer la conclusion

générale suivante : *Deux points correspondants dans une pseudosubstitution du second ordre sont conjugués par rapport au cercle de symétrie de la pseudosubstitution.*

Au lieu de dire de deux points qu'ils sont conjugués, nous dirons quelquefois qu'ils sont *symétriques;* et nous désignerons une pseudosubstitution du second ordre sous le nom de *réflexion* par rapport à son cercle de symétrie.

Projetons stéréographiquement le plan sur une sphère. Le cercle de symétrie de la réflexion, soit Γ, aura pour projection sur la sphère un cercle Γ_1. Soient z et z' deux points correspondants dans la réflexion considérée ; puisque z et z' sont conjugués par rapport à Γ, tout cercle passant par ces deux points est orthogonal à Γ, et, comme la projection stéréographique conserve les angles, les projections z_1, z'_1 de z, z' sur la sphère posséderont la même propriété relativement au cercle Γ_1.

Si en particulier Γ_1 est un grand cercle, les points z_1 et z'_1 seront symétriques par rapport à Γ_1, au sens ordinaire du mot. Donc, *supposons qu'on projette stéréographiquement une réflexion sur une sphère, de façon que le cercle de symétrie ait pour projection un grand cercle. Si nous considérons deux points du plan se correspondant dans la réflexion, leurs projections sur la sphère sont deux points symétriques* (au sens ordinaire du mot) *par rapport à ce grand cercle.*

42. Considérons maintenant une pseudosubstitution Q

$$z' = \frac{\alpha\bar{z} + \beta}{\gamma\bar{z} + \delta}$$

qui ne soit pas du second ordre. Posons

$$Q^2 = \begin{pmatrix} \alpha\bar{\alpha} + \beta\bar{\gamma} & \alpha\bar{\beta} + \beta\bar{\delta} \\ \gamma\bar{\alpha} + \delta\bar{\gamma} & \gamma\bar{\beta} + \delta\bar{\delta} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

La quantité

$$A + D = \alpha\bar{\alpha} + \beta\bar{\gamma} + \gamma\bar{\beta} + \delta\bar{\delta}$$

est évidemment réelle. Donc (nº 24) :

Le carré d'une pseudosubstitution n'est jamais une substitution loxodromique.

Suivant que la substitution Q^2 est *elliptique*, *hyperbolique* ou *parabolique*, on dit que la pseudosubstitution Q est elliptique, hyperbolique ou parabolique.

43. Comme on l'a déjà observé, les seuls points qu'une pseudosubstitution Q puisse laisser invariables sont les pôles de la substitution Q^2. Examinons dans quels cas il en est effectivement ainsi.

Désignons par p et q les deux pôles de Q^2, distincts ou non; on a (n° 23)

$$(1) \qquad \begin{matrix} p \\ q \end{matrix} \Big\} = \frac{A - D \pm \sqrt{(A + D)^2 - 4}}{2C},$$

en supposant, ce qui est toujours permis,

$$(2) \qquad \alpha\delta - \beta\gamma = 1,$$

d'où

$$\bar{\alpha}\bar{\delta} - \bar{\beta}\bar{\gamma} = 1,$$

$$AD - BC = (\alpha\delta - \beta\gamma)(\bar{\alpha}\bar{\delta} - \bar{\beta}\bar{\gamma}) = 1.$$

Si le point p n'est pas déplacé par Q, on doit avoir

$$p = \frac{\alpha\bar{p} + \beta}{\gamma\bar{p} + \delta}$$

ou bien

$$\gamma p\bar{p} + \delta p - \alpha\bar{p} - \beta = 0$$

qui peut encore s'écrire, en multipliant par γ et tenant compte de (2),

$$(3) \qquad (\gamma p - \alpha)(\gamma\bar{p} + \delta) = -1.$$

Pour reconnaître dans quelles conditions cette relation peut avoir lieu, il convient d'établir certaines identités.

On a tout d'abord

$$(4) \qquad A - \bar{D} = \bar{A} - D = \alpha\bar{\alpha} - \delta\bar{\delta}.$$

De plus, on trouve facilement

$$(5) \qquad \gamma A - \alpha C = \gamma\bar{D} - \delta\bar{C} = -\bar{\gamma}.$$

Cela posé, écrivons (1) sous la forme

$$\left.\begin{matrix} p \\ q \end{matrix}\right\} = \frac{A - D \pm R}{2C},$$

où R est nul, réel et différent de zéro ou imaginaire pur, suivant que la substitution Q est parabolique, hyperbolique ou elliptique.

Soit donc

$$p = \frac{A - D + R}{2C};$$

alors

$$\bar{p} = \frac{\bar{A} - \bar{D} \pm R}{2\bar{C}}.$$

Dans cette formule, où figure un double signe, on doit prendre le signe + si Q est hyperbolique, le signe — si Q est elliptique (si Q est parabolique, $R = \bar{R} = 0$, le signe est alors indifférent). Il suit de là

$$\gamma p - \alpha = \frac{1}{2C}(\gamma A - \gamma D - 2\alpha C + \gamma R),$$

$$\gamma \bar{p} + \delta = \frac{1}{2\bar{C}}(\gamma \bar{A} - \gamma \bar{D} + 2\delta \bar{C} \pm \gamma R).$$

En tenant compte de (4) et (5),

$$\begin{aligned} \gamma p - \alpha &= \frac{1}{2C}[\gamma A + \gamma(A - \bar{D} - \bar{A}) - 2\alpha C + \gamma R] \\ &= \frac{1}{2C}[2(\gamma A - \alpha C) - \gamma(\bar{A} + \bar{D}) + \gamma R] \\ &= \frac{1}{2C}[-2\bar{\gamma} - \gamma(A + D) + \gamma R], \end{aligned}$$

$$\begin{aligned} \gamma \bar{p} + \delta &= \frac{1}{2\bar{C}}[\gamma(A + D - \bar{D}) - \gamma \bar{D} + 2\delta \bar{C} \pm \gamma R] \\ &= \frac{1}{2\bar{C}}[-2(\gamma \bar{D} - \delta \bar{C}) + \gamma(A + D) \pm \gamma R] \\ &= \frac{1}{2\bar{C}}[2\bar{\gamma} + \gamma(A + D) \pm \gamma R]. \end{aligned}$$

Cette dernière relation peut s'écrire

$$\gamma \bar{p} + \delta = \frac{1}{2\bar{C}}[2\bar{\gamma} + \gamma(A + D) + \gamma R - 2\varepsilon R],$$

ε étant égal à o ou à γ, suivant que Q est hyperbolique ou elliptique. Il en résulte

$$(\gamma p - \alpha)(\gamma \bar{p} + \delta) = -\frac{1}{4C\bar{C}}\{[2\gamma + \gamma(A+D)]^2 - \gamma^2 R^2 - \varepsilon T\},$$

en désignant par T la quantité

$$-2R[-2\gamma - \gamma(A+D) + \gamma R].$$

En développant et se rappelant que $R = (A+D)^2 - 4$, on a

$$\begin{aligned}(\gamma p - \alpha)(\gamma \bar{p} + \delta) &= -\frac{1}{4C\bar{C}}[4\bar{\gamma}^2 + 4\bar{\gamma}\gamma(A+D) + 4\gamma^2 - \varepsilon T] \\ &= -\frac{1}{C\bar{C}}[\bar{\gamma}^2 + \bar{\gamma}\gamma(A+D) + \gamma^2] + \frac{\varepsilon T}{4C\bar{C}}.\end{aligned}$$

D'autre part,

$$\begin{aligned}C\bar{C} &= (\gamma\bar{\alpha} + \delta\bar{\gamma})(\bar{\gamma}\alpha + \bar{\delta}\gamma) \\ &= \alpha\bar{\alpha}\gamma\bar{\gamma} + \gamma^2\bar{\alpha}\bar{\delta} + \bar{\gamma}^2\alpha\delta + \gamma\bar{\gamma}\delta\bar{\delta} \\ &= \alpha\bar{\alpha}\gamma\bar{\gamma} + \gamma^2(\bar{\beta}\bar{\gamma} + 1) + \bar{\gamma}^2(\beta\gamma + 1) + \gamma\bar{\gamma}\delta\bar{\delta} \\ &= \gamma^2 + \bar{\gamma}^2 + \gamma\bar{\gamma}(A+D);\end{aligned}$$

d'où

$$(\gamma p - \alpha)(\gamma \bar{p} + \delta) = -1 + \frac{\varepsilon T}{4C\bar{C}}.$$

En comparant cette relation avec la relation (3), on voit que $\varepsilon = 0$. On arrive donc à la conclusion suivante : *Si* Q *est parabolique ou hyperbolique, il existe un ou deux points qu'elle laisse invariables : c'est le pôle ou bien les pôles de* Q^2 ; *si* Q *est elliptique, il n'en existe aucun.*

On peut ajouter que, *si* Q *est elliptique, elle échange entre eux les deux pôles de* Q^2.

Soient, en effet, p l'un de ces pôles et s ce qu'il devient par la substitution Q. Puisque p reste inaltéré par Q^2, c'est que Q doit changer s en p. Donc les deux points p, s sont échangés entre eux par Q. Mais alors Q^2 laisse évidemment s invariable et, par suite, s est le second pôle de Q^2.

44. *Étant donnée une substitution non loxodromique, si on la transforme par une réflexion relativement à une de ses tra-*

jectoires, la substitution transformée est égale à la substitution primitive.

Revenons au plan z des nᵒˢ 27 et 30. Une substitution P elliptique ou hyperbolique prend la forme

$$Z' = \theta Z.$$

Dans le premier cas $|\theta| = 1$; dans le second cas θ est une quantité réelle et positive.

Une réflexion R par rapport au cercle ayant pour rayon r et l'origine pour centre est de la forme

$$Z' = \frac{r^2}{\overline{Z}}.$$

Pour former le produit RPR, on doit éliminer Z′ et Z″ entre

$$Z' = \frac{r^2}{\overline{Z}}, \qquad Z'' = \theta Z', \qquad Z''' = \frac{r^2}{\overline{Z''}}.$$

En tenant compte de $|\theta| = 1$, on obtient

$$Z''' = \theta Z,$$

d'où

$$RPR = P.$$

Une réflexion R par rapport à un rayon d'argument α issu de l'origine a la forme

$$Z' = e^{2i\alpha}\overline{Z}.$$

Pour former le produit RPR, on doit éliminer Z′ et Z″ entre

$$Z' = e^{2i\alpha}\overline{Z}, \qquad Z'' = \theta Z', \qquad Z''' = e^{2i\alpha}\overline{Z''},$$

et, en tenant compte de ce que θ est réel et positif, on obtient

$$Z''' = \theta Z,$$

en sorte que

$$RPR = P.$$

Dans le cas d'une substitution parabolique

$$Z' = \eta + Z,$$

on peut toujours supposer que η est réel. Les trajectoires sont des

droites parallèles à l'axe réel, et la réflexion R par rapport à l'une d'elles, située à une distance h de cet axe, est

$$Z' = 2ih + \overline{Z}.$$

Éliminant Z' et Z'' entre

$$Z' = 2ih + \overline{Z}, \qquad Z'' = \eta + Z', \qquad Z''' = 2ih + \overline{Z''},$$

on obtient

$$Z''' = \eta + Z,$$

en sorte que, là encore, on a

$$\mathrm{RPR} = \mathrm{P}.$$

45. *Soit un groupe de substitutions* G *permutable* (n° 12) *avec une réflexion* R *et soit* P *un élément quelconque de* $\overline{\mathrm{G}}$; *les opérations* P, PR (*ou bien* P, RP) *constituent un groupe* G *dit groupe déduit de* G *par amplification.*

Si G est d'un ordre fini, $\overline{\mathrm{G}}$ est d'un ordre double.

Soient P_1, P_2 deux substitutions quelconques de G. Posons

$$\mathrm{RP_1R} = \mathrm{P}'_1, \qquad \mathrm{RP_2R} = \mathrm{P}'_2;$$

par hypothèse P'_1, P'_2 appartiennent aussi à G. Considérons les quatre produits

$$\mathrm{P_1P_2}, \quad \mathrm{P_1R.P_2}, \quad \mathrm{P_1.P_2R}, \quad \mathrm{P_1R.P_2R}.$$

Le premier est évidemment un élément de G. Le second, qui peut s'écrire $\mathrm{P_1P'_2R}$ ou bien $\mathrm{P_1P'_2.R}$, est de la forme PR. Il en est de même pour le troisième. Quant au quatrième on peut l'écrire

$$\mathrm{P_1.RP_2.R} \quad \text{ou} \quad \mathrm{P_1P'_2R^2}$$

ou enfin

$$\mathrm{P_1P'_2},$$

en sorte qu'il appartient à G.

L'existence du groupe $\overline{\mathrm{G}}$ est donc établie.

46. *Soit un groupe de substitutions* G (*fini ou infini*) *dont chacun des éléments peut être mis sous forme de produit de facteurs appartenant à un ensemble fini de substitutions* P_1,

$P_2, \ldots, P_r$. *Supposons qu'une réflexion* R *transforme chacune des substitutions précédentes en une substitution de* G, *alors le groupe* G *peut être amplifié par la réflexion* R.

Posons, en général,

$$RP_iR = P'_i \qquad (i = 1, 2, \ldots, r).$$

Si

$$P_{i_1}^{\alpha_1} P_{i_2}^{\alpha_2} P_{i_3}^{\alpha_3} \ldots,$$

où $i_1, i_2, i_3, \ldots$ sont des nombres, distincts ou non, appartenant à la suite $1, 2, 3, \ldots, r$, est une substitution quelconque de G, on trouve facilement

$$RP_{i_1}^{\alpha_1} P_{i_2}^{\alpha_2} P_{i_3}^{\alpha_3} \ldots R = P'^{\alpha_1}_{i_1} P'^{\alpha_2}_{i_2} P'^{\alpha_3}_{i_3} \ldots,$$

ce qui démontre le théorème :

47. *Si* P *désigne la substitution à pôles distincts* p, q

$$\frac{z'-p}{z'-q} = \theta \frac{z-p}{z-q}$$

et Q *la pseudosubstitution*

$$z' = \frac{\alpha \bar{z} + \beta}{\gamma \bar{z} + \delta},$$

la substitution $Q^{-1}PQ = P'$ *a pour expression*

$$\frac{z'-p'}{z'-q'} = \bar{\theta} \frac{z-p'}{z-q'},$$

où p' *et* q' *ont pour valeur*

$$p' = \frac{\alpha \bar{p} + \beta}{\gamma \bar{p} + \delta}, \qquad q' = \frac{\alpha \bar{q} + \beta}{\gamma \bar{q} + \delta}.$$

En effet, en éliminant z' et z'' entre

$$z = \frac{\alpha \bar{z}' + \beta}{\gamma \bar{z}' + \delta}, \qquad \frac{z''-p}{z''-q} = \theta \frac{z'-p}{z'-q}, \qquad z''' = \frac{\alpha \bar{z}'' + \beta}{\gamma \bar{z}'' + \delta},$$

on obtient

$$\frac{\dfrac{\bar{\delta} \bar{z}''' - \bar{\beta}}{-\bar{\gamma} \bar{z}''' + \bar{\alpha}} - p}{\dfrac{\bar{\delta} \bar{z}''' - \bar{\beta}}{-\bar{\gamma} \bar{z}''' + \bar{\alpha}} - q} = \theta \frac{\dfrac{\bar{\delta} \bar{z} - \bar{\beta}}{-\bar{\gamma} \bar{z} + \bar{\alpha}} - p}{\dfrac{\bar{\delta} \bar{z} - \bar{\beta}}{-\bar{\gamma} \bar{z} + \bar{\alpha}} - q}$$

ou bien

$$\frac{\bar{z}''' - \dfrac{\bar{\alpha} p + \bar{\beta}}{\bar{\gamma} p + \bar{\delta}}}{\bar{z}''' - \dfrac{\bar{\alpha} q + \bar{\beta}}{\bar{\gamma} q + \bar{\delta}}} = \theta \frac{\bar{z} - \dfrac{\bar{\alpha} p + \bar{\beta}}{\bar{\gamma} p + \bar{\delta}}}{\bar{z} - \dfrac{\bar{\alpha} q + \bar{\beta}}{\bar{\gamma} q + \bar{\delta}}}$$

et, prenant les conjugués des deux membres,

$$\frac{z''' - \dfrac{\alpha \bar{p} + \beta}{\gamma \bar{p} + \delta}}{z''' - \dfrac{\alpha \bar{q} + \beta}{\gamma \bar{q} + \delta}} = \bar{\theta} \frac{z - \dfrac{\alpha \bar{p} + \beta}{\gamma \bar{p} + \delta}}{z - \dfrac{\alpha \bar{q} + \beta}{\gamma \bar{q} + \delta}},$$

on peut donc dire que :

a. Les pôles de P′ sont les transformés par Q des pôles de P.

b. Si P est hyperbolique, il en est de même de P′ et les deux substitutions ont le même coefficient θ.

c. Si P est elliptique, il en est de même de P′, et dans les deux substitutions les coefficients θ sont conjugués.

48. *Si* P *est la substitution à pôle unique*

$$\frac{1}{z' - r} = \eta + \frac{1}{z - r}$$

et Q *la pseudosubstitution*

$$z' = \frac{\alpha \bar{z} + \beta}{\gamma \bar{z} + \delta},$$

où l'on suppose $\alpha\delta - \beta\gamma = 1$, *l'expression de la substitution* $Q^{-1}PQ = P'$ *est*

$$\frac{1}{z' - r'} = \eta' + \frac{1}{z - r'},$$

r' *et* η' *ayant pour valeurs*

$$r' = \frac{\alpha \bar{r} + \beta}{\gamma \bar{r} + \delta}, \qquad \eta' = \bar{\eta}(\gamma \bar{r} + \delta)^2.$$

Éliminant z' et z'' entre

$$z = \frac{\alpha \bar{z}' + \beta}{\gamma \bar{z}' + \delta}, \qquad \frac{1}{z'' - r} = \eta + \frac{1}{z' - r}, \qquad z''' = \frac{\alpha \bar{z}'' + \beta}{\gamma \bar{z}'' + \delta},$$

on obtient

$$\frac{1}{\dfrac{\bar{\delta}\bar{z}''' - \bar{\beta}}{-\bar{\gamma}\bar{z}''' + \bar{\alpha}} - r} = \eta + \frac{1}{\dfrac{\bar{\delta}\bar{z} - \bar{\beta}}{-\bar{\gamma}\bar{z} + \bar{\alpha}} - r}$$

ou bien, en utilisant les réductions du n° 32,

$$\frac{1}{\bar{z}''' - \dfrac{\bar{\alpha} r + \bar{\beta}}{\bar{\gamma} r + \bar{\delta}}} = \eta(\bar{\gamma} r + \bar{\delta})^2 + \frac{1}{\bar{z} - \dfrac{\bar{\alpha} r + \bar{\beta}}{\bar{\gamma} r + \bar{\delta}}},$$

ou, prenant enfin les conjugués des deux membres,

$$\frac{1}{z''' - \dfrac{\alpha \bar{r} + \beta}{\gamma \bar{r} + \delta}} = \bar{\eta}(\gamma \bar{r} + \delta)^2 + \frac{1}{z - \dfrac{\alpha \bar{r} + \beta}{\gamma \bar{r} + \delta}}.$$

Groupes finis de rotations d'une sphère sur elle-même et leur amplification.

49. Nous venons d'établir les propriétés des substitutions et pseudosubstitutions linéaires. Passons maintenant à l'étude des groupes de substitutions, particulièrement des groupes finis, et des groupes de substitutions amplifiés.

Le seul groupe infini que nous rencontrerons est le groupe *modulaire*, dont nous donnerons plus loin une définition arithmétique directe.

Quant aux groupes finis de substitutions, nous en obtiendrons très facilement la construction, grâce à un artifice géométrique utilisé déjà précédemment (n° 28).

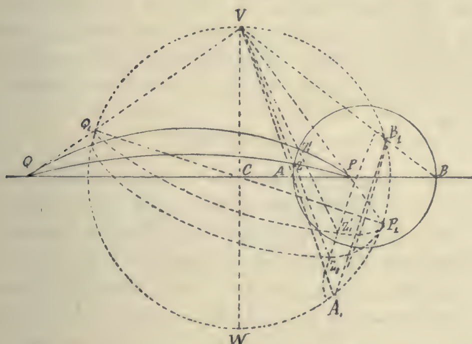
Rappelons que les groupes finis ne comprennent que des substitutions elliptiques (n° 33).

Soit donc une substitution elliptique, dont les pôles p et q soient représentés par les points P et Q. Considérons la famille des cercles Γ admettant P et Q pour points conjugués. La substitution considérée laisse invariable chaque cercle Γ. Elle change un point Z d'un tel cercle en un autre point Z′ du même cercle, tel que la différence des angles QZ′P et QZP reste constante (n° 29).

Considérons le plan passant par P et Q et perpendiculaire au

plan z; soient V un point de ce plan, tel que le plan PVQ soit droit, et C le pied de la perpendiculaire abaissée de V sur le plan z. Projetons stéréographiquement le plan z sur la sphère décrite de C comme centre avec CV pour rayon, en prenant V pour point de vue, et soit M_1 la projection stéréographique d'un point quelconque M du plan z (¹).

Fig. 2.



Le point C étant situé sur PQ, le plan VPQ passe par le centre de la sphère, les points P_1, Q_1 se trouvent sur un grand cercle passant par V (contour apparent de la sphère), et, comme l'angle PVQ est droit, $P_1 Q_1$ est un diamètre de la sphère. Soient A et B les points de rencontre de la droite PQ avec l'un des cercles Γ. Les quatre points P, Q, A, B forment une division harmonique, le faisceau V(PQAB) est harmonique et les deux droites rectangulaires VP, VQ sont les bissectrices des angles formés par VA et VB. Donc P_1 est le milieu de l'arc $A_1 B_1$, la droite $A_1 B_1$ est perpendiculaire à la droite $P_1 Q_1$, et la projection stéréographique du cercle AB est un cercle $A_1 B_1$ situé dans un plan perpendiculaire au diamètre $P_1 Q_1$.

Pour la substitution considérée

$$\frac{z'-p}{z'-q} = \theta \frac{z-p}{z-q} = e^{i\alpha} \frac{z-p}{z-q}, \tag{1}$$

(¹) Dans la figure on a tracé en traits pleins les lignes du plan z.

un point Z du cercle AB se transforme en un autre point Z′ du même cercle, tel que les arcs de cercle PZQ, PZ′Q fassent entre eux l'angle α. Les arcs PZQ, PZ′Q se projettent sur la sphère suivant les demi-grands cercles $P_1 Z_1 Q_1$, $P_1 Z'_1 Q_1$ dont les plans font le même angle α, puisque la projection stéréographique conserve les angles.

Donc, à la substitution linéaire considérée correspond sur la sphère une rotation d'amplitude α autour du diamètre $P_1 Q_1$. On peut dire que les points P_1, Q_1 sont les *pôles* de la rotation.

Pour déterminer le sens de cette rotation, examinons le cas particulier où $p = 0$, $q = \infty$. Alors, la substitution prend la forme plus simple

$$z' = \theta z = e^{i\alpha} z$$

et représente une rotation du plan, sur lui-même, d'un angle α autour de l'origine, effectuée dans le sens qui va de l'axe des x positifs vers l'axe des y positifs, c'est-à-dire de gauche à droite. Il lui correspond une rotation d'angle α, de la sphère sur elle-même, de gauche à droite autour de l'axe VW. Mais puisque, dans le cas spécial considéré, P_1 coïncide avec W et Q_1 avec V, on peut dire qu'on a une rotation de la sphère d'angle α effectuée de droite à gauche autour de l'axe $P_1 Q_1$ (¹).

Si donc on considère comme positives les rotations effectuées de droite à gauche, on peut dire qu'à la substitution (1) correspond une rotation de la sphère d'angle α autour de l'axe $P_1 Q_1$.

Il importe de faire la remarque suivante : tandis que la transformation du plan z en lui-même par la substitution (1) est accompagnée en général d'une déformation, la transformation correspondante de la sphère en elle-même est tout simplement une rotation de cette sphère autour d'un de ses diamètres.

50. On sait que la succession de deux rotations autour de deux axes ayant un point commun équivaut à une rotation unique autour d'un axe passant par ce point. Donc les rotations d'une sphère sur elle-même forment un groupe. Un quelconque des sous-groupes du groupe précédent peut être considéré comme

(¹) Une telle rotation s'effectue de droite à gauche pour un observateur placé les pieds en Q_1 et la tête en P_1.

l'image d'un groupe de substitutions linéaires elliptiques [1] auquel il est holoédriquement isomorphe ou, ce qui revient au même, auquel il est identique au point de vue formel.

Montrons maintenant comment on peut construire les groupes finis de rotations correspondant aux groupes de substitutions linéaires du Tableau (nº 37); nous aurons ainsi démontré l'existence effective de tous les groupes dont nous avions seulement établi la possibilité d'existence.

Un premier type de groupes finis de rotations est celui des groupes cycliques (nº 6), formés chacun d'une rotation, dont l'amplitude est dans un rapport commensurable avec 2π et par les puissances de cette rotation. Si ce rapport, réduit à sa plus simple expression, est $\frac{k}{n}$, le groupe est d'ordre n; nous le représenterons par C_n.

Chacun des deux pôles communs à toutes les rotations du groupe n'est équivalent qu'à lui-même, puisque le groupe ne contient aucune rotation, échangeant entre eux les deux pôles. On a donc (avec les notations du nº 37)

$$r = 2, \qquad \frac{n}{\nu_1} = 1, \qquad \frac{n}{\nu_2} = 1$$

et, par suite,

$$\nu_1 = \nu_2 = n.$$

Les groupes cycliques correspondent par conséquent au type I *du Tableau.*

51. Pour construire les autres groupes finis, nous nous reporterons aux polyèdres réguliers que nous imaginerons inscrits dans la sphère. Mais, outre les cinq solides réguliers que nous appellerons *polyèdres proprement dits,* nous devrons en considérer un sixième, pour ainsi dire dégénéré, formé de deux faces polygonales régulières confondues et que nous appellerons *dièdre.* Il sera considéré comme inscrit dans la sphère, si le polygone régulier correspondant est inscrit dans un grand cercle de la sphère : alors

---

[1] Les pôles de ces substitutions ne peuvent avoir la même disposition que dans le plan. En effet, si P et Q sont les pôles d'une quelconque d'entre elles, il doit exister un point V tel que les plans PVQ soient perpendiculaires au plan z et que les angles PVQ soient nuls.

le diamètre perpendiculaire au plan de ce grand cercle s'appellera l'*axe* du dièdre.

Si le polygone a m côtés, le dièdre sera dit *m-gonal.* Pour $m = 2$, on a un degré encore plus avancé de dégénérescence; le dièdre se réduit simplement à un segment de droite que nous regarderons comme inscrit dans la sphère, puisqu'il coïncide avec l'un des diamètres. Dans ce cas, tout diamètre perpendiculaire au précédent devrait être regardé comme axe du dièdre. Cependant nous ne réserverons cette dénomination qu'à un seul diamètre, car nous supposerons que le polygone constituant le dièdre ait été réduit par continuité à un couple de segments confondus, et cela tout en restant dans un plan déterminé, et c'est ce plan qu'on regardera à la limite comme le plan du polygone dégénéré. Il existe une rotation et une seule faisant coïncider AB avec CD, et il en est de même pour AB et DC (¹).

Or, toute rotation de la sphère qui amène deux arêtes en coïncidence laisse le polyèdre invariable, et réciproquement toute rotation qui laisse le polyèdre inaltéré réalise la coïncidence de chaque arête avec une autre arête. On aura, par suite, l'ensemble des rotations qui transforment un polyèdre en lui-même en choisissant une arête déterminée et prenant dans les deux sens possibles toutes les rotations qui amènent cette arête en coïncidence avec elle-même et les autres arêtes.

Si donc A désigne le nombre des arêtes, il existe 2 A rotations, y compris la rotation nulle, qui transforment le polyèdre en lui-même. Ces rotations forment évidemment un groupe, car, si deux rotations possèdent la propriété indiquée, il en est de même encore de leur produit. Donc :

Les rotations qui transforment en lui-même un polyèdre régulier constituent un groupe fini, dont l'ordre est égal au double du nombre des arêtes du polyèdre.

Il en résulte qu'aux six polyèdres réguliers (y compris le dièdre) correspondent six groupes finis de rotations de la sphère sur elle-même.

(¹) *Voir*, par exemple, MARCOLONGO, *Mécanique rationnelle*, t. I, p. 59 et suiv. Milan, Hœpli, 1905.

Cependant ces groupes ne sont pas tous distincts.

Soient, en effet, un polyèdre régulier proprement dit inscrit dans une sphère et le polyèdre conjugué, c'est-à-dire le polyèdre ayant pour sommets les centres sphériques des faces du premier. Il est clair que, si le polyèdre primitif reste inaltéré par une certaine rotation, il en est de même du polyèdre conjugué, et que par suite les deux polyèdres admettent le même groupe de rotations. D'autre part, le tétraèdre, l'octaèdre et l'icosaèdre ayant respectivement pour conjugués le tétraèdre, l'hexaèdre et le dodécaèdre réguliers, les polyèdres réguliers donneront lieu aux groupes suivants de rotations, dont l'ordre se déduit immédiatement du nombre des arêtes du polyèdre générateur :

a. Le groupe *diédrique* d'ordre $n = 2m$, m étant le nombre des côtés du polygone formant le dièdre;

b. Le groupe *tétraédrique* d'ordre $n = 12$;

c. Le groupe *octaédrique* ou *hexaédrique* d'ordre $n = 24$;

d. Le groupe *icosaédrique* ou *dodécaédrique* d'ordre $n = 60$.

Nous nous proposons d'étudier séparément chacun de ces groupes.

52. Étant donné un polyèdre régulier, projetons-le sur la surface sphérique circonscrite, en prenant comme point de vue le centre de la sphère. Nous obtenons ainsi un réseau de polygones sphériques réguliers recouvrant toute la sphère. Pour la commodité du langage, nous désignerons encore cette figure sous le nom de *polyèdre* [1]; alors les faces, les arêtes et les sommets de ce polyèdre désigneront, pour les polygones sphériques ainsi tracés, leurs arêtes et leurs sommets.

Cherchons maintenant les rotations laissant ce polyèdre inaltéré.

Si le pôle d'une telle rotation ne se trouve pas sur une arête, il est situé nécessairement au centre d'une face; car autrement une rotation ayant ce point comme pôle ne pourrait changer cette face ni en elle-même, ni en une autre face.

---

[1] Dans les cas pouvant donner lieu à équivoque, nous dirons *polyèdre sphérique* au lieu de polyèdre.

Si le pôle, sans être un sommet, est situé sur une arête, il est clair qu'il doit se trouver au milieu de cette arête.

Ces considérations montrent que les seules rotations changeant le polyèdre en lui-même sont les suivantes :

1° Rotations ayant pour pôles les milieux des arêtes; leur amplitude est π;

2° Rotations ayant pour pôles les centres des faces; leur amplitude est $\frac{2\pi}{f}$ et ses multiples, f désignant le nombre des côtés appartenant à chaque face;

3° Rotations ayant pour pôles les sommets; leur amplitude est $\frac{2\pi}{q}$ et ses multiples, q désignant le nombre des arêtes aboutissant à chaque sommet.

Dans chaque catégorie, les pôles sont équivalents entre eux, car il existe toujours des rotations qui échangent deux arêtes, deux faces ou deux sommets quelconques.

Si l'on désigne par A, F, S le nombre des arêtes, des faces et des sommets du polyèdre, le nombre des pôles est respectivement dans les trois cas précédents A, F, S. D'autre part, si chacun des pôles des trois catégories est commun à ν_1, ν_2, ν_3 rotations, le nombre des pôles eux-mêmes est respectivement (n° 36) $\frac{n}{\nu_1}$, $\frac{n}{\nu_2}$, $\frac{n}{\nu_3}$; d'où

$$(1) \qquad \frac{n}{\nu_1} = \text{A}, \qquad \frac{n}{\nu_2} = \text{F}, \qquad \frac{n}{\nu_3} = \text{S},$$

et (n° 51), tenant compte de

$$(2) \qquad n = 2\text{A}$$

et de la relation (2) du n° 37, il vient

$$(3) \qquad \text{F} + \text{S} = \text{A} + 2,$$

qui est la *formule* d'Euler bien connue.

Les nombres ν_1, ν_2, ν_3 se déterminent facilement.

Tout d'abord, la comparaison des relations

$$\frac{n}{\nu_1} = \text{A}, \qquad n = 2\text{A}$$

donne $\nu_1 = 2$, comme on peut le voir aussi directement, car le

milieu d'une arête est un pôle pour deux rotations seulement : la rotation nulle et la rotation d'amplitude π.

Pour le dièdre $F = 2$, $A = m$, et, comme $n = 2m$, on trouve

$$\nu_2 = m, \quad \nu_3 = 2.$$

Considérons maintenant simultanément le tétraèdre, l'octaèdre et l'icosaèdre, qui possèdent la propriété commune d'avoir leurs faces triangulaires.

Le centre d'une quelconque de ces faces est un pôle pour trois rotations : la rotation nulle et deux autres, d'amplitudes $\frac{2\pi}{3}$, $\frac{4\pi}{3}$; d'où $\nu_2 = 3$.

Un sommet est un pôle pour la rotation nulle et $q - 1$ autres rotations d'amplitudes $\frac{2\pi}{q}$, $\frac{4\pi}{q}$, ..., $\frac{2(q-1)\pi}{q}$, q ayant ici la même signification que plus haut, en sorte que $\nu_3 = q$. Or, dans les trois cas, $q = 3, 4, 5$; par suite, $\nu_3 = 3, 4, 5$.

La formule

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} = 1 + \frac{2}{n}$$

devient alors

$$\frac{2}{n} = \frac{1}{q} - \frac{1}{6}$$

et par suite, dans les trois cas, $n = 12, 24, 60$, comme on pourrait d'ailleurs le déduire de la relation $n = 2S$.

Les formules précédentes donnent pour les trois polyèdres à faces triangulaires les relations suivantes entre F, A et S :

$$F = 2S - 4, \quad A = 3S - 6.$$

Comparant les résultats obtenus avec ceux du Tableau (n° 37), on voit que *les groupes diédriques, tétraédriques, octaédriques et icosaédriques correspondent respectivement aux cas* II, III, IV *et* V *de ce Tableau.*

Donc *les groupes que nous avons démontré être les seuls possibles existent bien réellement.*

53. Nous pouvons maintenant déterminer la structure des quatre groupes polyédriques, que nous représenterons toujours par les

symboles II, III, IV, V du Tableau connu, tandis que le symbole I désignera les groupes cycliques.

II. Les éléments du groupe diédrique sont :

La rotation identique;

Les $m-1$ rotations autour de l'axe du dièdre, d'amplitudes

$$\frac{2\pi}{m}, \quad \frac{4\pi}{m}, \quad \ldots, \quad \frac{2(m-1)\pi}{m};$$

Les m rotations d'amplitude π autour des m axes de symétrie du polygone, formant le dièdre.

Dans le cas de $m=2$, le groupe (*Vierergruppe*) que nous appellerons *groupe rectangulaire* comprend la rotation identique et trois rotations d'amplitude π autour de trois axes rectangulaires [1].

III. Les éléments du groupe tétraédrique sont :

La rotation identique ;

Les rotations d'amplitude π ayant pour pôles les milieux des six arêtes; comme de tels points sont deux à deux diamétralement opposés, il y a 3 rotations;

Les 4 rotations d'amplitude $\frac{2\pi}{3}$ et les 4 rotations d'amplitude $\frac{4\pi}{3}$ ayant chacune pour pôles le centre d'une face et le sommet opposé.

IV. Les éléments du groupe octaédrique sont :

La rotation identique;

Les rotations d'amplitude π ayant pour pôles les milieux des 12 arêtes; comme ces points sont deux à deux diamétralement opposés, il y a 6 rotations;

Les rotations d'amplitudes $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ ayant pour pôles les centres

---

[1] A ces rotations on devrait ajouter celles en nombre infini d'amplitude quelconque autour du diamètre auquel se réduit le dièdre. Mais on ne les considère pas comme transformant le dièdre en lui-même, à cause de la convention faite au n° 51, par laquelle le dièdre bigonal est regardé comme situé dans un plan déterminé.

des 8 faces; comme ces points sont deux à deux diamétralement opposés, il y a 8 rotations;

Les rotations d'amplitudes $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ ayant pour pôles les 6 sommets; et comme ces sommets sont diamétralement opposés, il y a 9 rotations.

V. Les éléments du groupe icosaédrique sont :

La rotation identique;

Les rotations d'amplitude π ayant pour pôles les milieux des 30 arêtes; pour des raisons vues précédemment, il y a 15 rotations:

Les 20 rotations d'amplitude $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ ayant pour pôles les centres des 20 faces;

Les 24 rotations d'amplitude $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$ ayant pour pôles les 12 sommets.

54. Occupons-nous maintenant de deux questions importantes concernant ces groupes, et recherchons :

a. S'ils sont simples ou composés (n° 15);

b. S'ils sont amplifiables (n° 45).

I. Un groupe cyclique, dont l'ordre est un nombre premier, est simple (*cf.* note, page 71).

Soit, au contraire, un groupe cyclique

$$1, \quad P, \quad P^2, \quad \ldots, \quad P^{n-1}$$

dont l'ordre n ne soit pas un nombre premier. Posons $n = rs$; le sous-groupe

$$1, \quad P^r, \quad P^{2r}, \quad \ldots, \quad P^{(s-1)r}$$

est invariant, puisque toutes les opérations du groupe donné sont permutables. Donc, si l'ordre d'un groupe cyclique n'est pas premier, le groupe est composé.

II. Le groupe diédrique d'ordre $n = 2m$ admet comme sous-groupe invariant le groupe cyclique des m rotations (y compris la rotation nulle) autour de l'axe du dièdre.

En effet, toute autre rotation du groupe échange entre eux les

pôles de ce sous-groupe et par suite transforme le sous-groupe en lui-même.

III. Le groupe tétraédrique admet comme sous-groupe invariant le groupe trirectangle formé de la rotation nulle et des rotations d'amplitude autour des trois méridiens, deux à deux rectangulaires.

En effet, toute autre rotation du groupe échange entre elles les trois médianes et, par suite, également les trois rotations d'amplitude n.

IV. Le groupe octaédrique, nous l'avons vu, laisse inaltéré un certain cube dont les sommets non consécutifs appartiennent à un tétraèdre régulier et les quatre autres au tétraèdre conjugué.

Toute rotation du groupe ne peut évidemment produire que l'un des deux effets suivants : ou bien laisser inaltéré chacun des deux tétraèdres, ou bien les échanger entre eux.

On peut établir que, sur les 24 rotations du groupe, 12 d'entre elles donnent lieu au premier effet et les 12 autres au second.

Soient $P_1, P_2, \ldots, P_l$ les rotations d'une de ces deux catégories et Q une rotation échangeant les deux tétraèdres. Les opérations $P_1 Q, P_2 Q, \ldots, P_l Q$ seront toutes distinctes et appartiendront à l'autre catégorie. Donc, le nombre d'éléments appartenant à l'une quelconque des deux catégories ne peut être inférieur au nombre des éléments de l'autre; en d'autres termes, les deux catégories renferment le même nombre d'éléments.

Les 12 rotations qui laissent inaltéré chacun des deux tétraèdres constituent un sous-groupe tétraédrique Γ. Je dis que ce sous-groupe est invariant. En effet, soient P une rotation de Γ et Q une rotation quelconque du groupe octaédrique n'appartenant pas à Γ; la rotation $Q^{-1}PQ$ laisse évidemment invariables les deux tétraèdres; donc elle appartient à Γ et l'on peut écrire

$$Q^{-1}\Gamma Q = \Gamma.$$

On peut aussi observer que le groupe trirectangle est un sous-groupe invariant du groupe octaédrique. En effet, toute rotation du groupe octaédrique laisse inaltérés les deux tétraèdres ou les échange entre eux, et, comme ces tétraèdres ont les médianes communes, toute rotation du groupe trirectangle échange entre elles ces médianes, d'où la conclusion annoncée.

V. Le groupe icosaédrique ne contient aucun sous-groupe invariant et par conséquent est un groupe simple.

Voici comment on peut le démontrer.

Le groupe icosaédrique G renferme, outre l'identité, 15 rotations d'ordre 2, 20 d'ordre 3, 24 d'ordre 5. Les pôles des rotations appartenant à chacune de ces trois espèces sont équivalents (n° 52), de sorte que les rotations d'une quelconque des trois espèces, ou bien sont les puissances d'une certaine rotation de la même espèce, ou bien s'obtiennent en transformant de telles puissances par des opérations convenables du groupe. Admettons qu'il existe un sous-groupe invariant Γ. Si Γ contient une rotation d'une certaine espèce, il contiendra toutes les rotations de la même espèce. Donc l'ordre de Γ sera représenté par un nombre de la forme

$$m = 1 + 15\alpha + 20\beta + 24\gamma,$$

α, β, γ ne pouvant prendre que les valeurs 0, 1; de plus, m doit être un diviseur de 60.

Nous laissons de côté les solutions

$$\alpha = \beta = \gamma = 1, \qquad \alpha = \beta = \gamma = 0,$$

qui correspondent respectivement à

$$\Gamma = G, \qquad \Gamma = 1.$$

Si $\gamma = 1$, alors $m \geqq 25$ et par suite nécessairement $m = 30$, d'où la relation

$$15\alpha + 20\beta = 30 - 1 - 24 = 5,$$

à laquelle il est impossible de satisfaire.

Soit donc $\gamma = 0$, d'où

$$m = 1 + 15\alpha + 20\beta.$$

On voit que m ne peut être multiple de 5, et comme le plus grand diviseur de 60, qui ne soit pas multiple de 5, est 12, on aurait $m \leqq 12$, ce qui est impossible si α et β ne sont pas nuls en même temps.

Donc le groupe icosaédrique ne contient aucun sous-groupe invariant.

55. Abordons maintenant la question de l'amplification des groupes considérés.

Prenons un polyèdre sphérique quelconque et considérons l'une quelconque de ses arêtes; le polyèdre est évidemment symétrique par rapport au grand cercle γ_1 contenant cette arête. Soient R la réflexion par rapport au cercle γ_1 et P une rotation quelconque du groupe G correspondant au polyèdre. Si (nos 41, 47) les pôles de P sont situés au milieu des arêtes, au centre des faces ou aux sommets du polyèdre, il en sera de même pour les pôles de $P' = RPR$; les rotations P, P' auront la même amplitude et seront de sens contraires (θ et $\bar{\theta}$ étant conjugués).

Il résulte de là que P' appartient au groupe G et que G est permutable avec la réflexion R.

Outre les cercles contenant les arêtes, le polyèdre peut avoir d'autres cercles de symétrie; par exemple, les cercles contenant les bissectrices des différentes faces ([1]), au sujet desquels on peut répéter tout ce qui vient d'être dit.

Donc :

Un groupe polyédrique est permutable avec toutes les réflexions, admettant pour cercles de symétrie les cercles du polyèdre correspondant.

D'où (n° 45) la conséquence suivante :

Un groupe polyédrique peut être amplifié par une réflexion relative à un quelconque des cercles de symétrie du polyèdre correspondant.

Nous verrons un peu plus loin que, quelle que soit la réflexion choisie, le groupe amplifié ainsi obtenu est toujours le même.

56. Étant donné un polyèdre sphérique, imaginons qu'on ait tracé tous ses cercles de symétrie. Ceux-ci contenant les médianes des différentes faces divisent chacune des faces en $2f$ triangles, alternativement égaux et symétriques ([2]), f étant le nombre des

---

([1]) Ces cercles sont distincts des précédents dans le dièdre et dans l'octaèdre; ils se confondent avec les précédents dans le tétraèdre et l'icosaèdre.

([2]) Dans les cas du dièdre et du tétraèdre les triangles, étant isoscèles, sont en même temps égaux et symétriques.

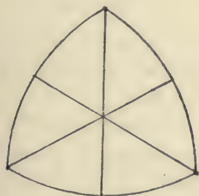
côtés de chaque face. On partage ainsi la surface sphérique en un réseau de triangles; quatre d'entre eux s'appuient sur chaque arête, et, comme il y a (n° 51) $\frac{n}{2}$ arêtes, ces triangles sont au nombre de $2n$. Donc :

Les cercles de symétrie d'un polyèdre divisent la sphère en $2n$ triangles alternativement égaux et symétriques, n désignant l'ordre du groupe polyédrique correspondant.

Tous ces triangles ont les mêmes angles égaux à $\frac{\pi}{\nu_1}$, $\frac{\pi}{\nu_2}$, $\frac{\pi}{\nu_3}$.

En effet, les trois sommets de chacun d'eux coïncident respectivement avec le milieu d'une arête, le centre d'une face et un des

Fig. 3.



sommets du polyèdre. Or, au premier de ces sommets correspond évidemment un angle droit; et comme on a toujours $\nu_1 = 2$, l'amplitude de l'angle est $\frac{\pi}{\nu_1}$.

Au second sommet, l'angle est $\frac{2\pi}{2f}$ ou $\frac{\pi}{f}$; or, pour le dièdre $f = m = \nu_2$ et pour les autres polyèdres $f = 3 = \nu_3$; l'amplitude de l'angle est donc $\frac{\pi}{\nu_2}$.

Enfin, au troisième sommet l'angle est $\frac{2\pi}{2q}$ ou $\frac{\pi}{q}$, q désignant (n° 52) le nombre des arêtes aboutissant à chaque sommet. Or, pour le dièdre $q = 2 = \nu_3$, pour les autres polyèdres $q = \nu_3$, donc l'amplitude de l'angle est $\frac{\pi}{\nu_3}$ [1].

---

[1] La formule connue de l'aire d'un triangle sphérique nous donne une vérifi-

57. Toute rotation de la sphère qui laisse le polyèdre inaltéré fait coïncider un des $2n$ triangles du réseau avec un autre triangle égal. Mais, à l'exception de la rotation nulle, aucune rotation n'amène un triangle à coïncider avec lui-même ; donc, étant donnés deux triangles égaux, il existe au plus une rotation du groupe qui amène l'un d'eux en coïncidence avec l'autre. Cette rotation existe effectivement, car, si pour un certain couple de triangles elle n'existait pas, le nombre des rotations du groupe serait inférieur à celui des triangles égaux, tandis qu'en réalité ces deux nombres sont les mêmes.

Donc :

Étant donnés deux triangles égaux du réseau, il existe une rotation du groupe et une seule qui amène l'un d'eux en coïncidence avec l'autre.

Pour plus de clarté, imaginons qu'on couvre de hachures les n triangles égaux de l'un des systèmes et qu'on laisse en blanc les n triangles de l'autre système.

Prenons arbitrairement l'un des triangles blancs comme premier triangle et faisons-lui correspondre la rotation nulle. Faisons correspondre à chaque triangle blanc la rotation qui amène ensuite le premier triangle blanc en coïncidence avec lui ; nous aurons par là même établi une correspondance biunivoque entre les n triangles blancs et les n rotations du groupe.

Maintenant, quel est le rôle des triangles ombrés dans ce mode de représentation ?

Une réflexion par rapport à l'un quelconque des cercles du réseau fait coïncider la figure avec elle-même, mais transforme chaque triangle blanc en un triangle ombré, et réciproquement.

---

cation du résultat obtenu. L'aire d'un triangle du réseau et son excès sphérique ont respectivement pour valeurs

$$\frac{4\pi}{2n} = \frac{2\pi}{n}$$

et

$$\frac{\pi}{\nu_1} + \frac{\pi}{\nu_2} + \frac{\pi}{\nu_3} - \pi = \left(\sum_{i=1}^{3} \frac{1}{\nu i} - 1\right).$$

En égalant ces deux expressions, on obtient la formule (2) (n° 37).

Le même fait se produit pour une rotation, suivie d'une réflexion, et il est facile de voir que, si l'on fixe arbitrairement un triangle blanc et un triangle ombré, il existe une rotation et une seule dont le produit par une réflexion déterminée amène le premier triangle en coïncidence avec le second. Si donc on choisit arbitrairement un triangle blanc et qu'on le considère comme correspondant à l'opération identique, on peut établir une correspondance biunivoque entre les $2n$ triangles du réseau et les $2n$ opérations du groupe amplifié : il suffit de faire correspondre à chacun des triangles l'opération par laquelle le triangle primitivement choisi vient coïncider avec lui.

On voit bien maintenant que, quelle que soit la réflexion choisie, le groupe amplifié est toujours le même.

Voici à propos du réseau précédent une observation importante : *étant donné un triangle du réseau, on peut en déduire par symétrie le réseau tout entier*. Pour cela, on construit d'abord les triangles symétriques du premier par rapport à ses trois côtés ; on répète ensuite la même opération sur chacun des nouveaux triangles obtenus, et ainsi de suite.

58. Si simple que soit la représentation sphérique des groupes précédents, il est évidemment préférable, pour des raisons d'ordre pratique, de lui substituer une représentation plane. On y parvient très simplement à l'aide de la projection stéréographique. En vertu d'une propriété souvent rappelée, nous obtiendrons des figures composées exclusivement de droites ou de cercles, donc d'une construction facile. Nous ferons un peu plus loin une étude spéciale des figures de ce genre ; pour l'instant, bornons-nous à observer qu'*elles peuvent être déduites d'un triangle unique au moyen d'une symétrie*, le mot *symétrie* ayant la même signification qu'au n° 41.

Construction des groupes finis de substitutions et de leurs groupes amplifiés.

59. Nous avons vu (n° 49) comment, moyennant une projection stéréographique appropriée, il est possible de déduire d'une substitution linéaire elliptique une rotation de la sphère sur elle-même

Réciproquement, étant donné un groupe fini de rotations d'une sphère sur elle-même, on en déduit, à l'aide d'une projection stéréographique sur le plan de la variable complexe, un groupe fini de substitutions. Nous avons montré (nos 40 et suivants) que les groupes polyédriques sont susceptibles de nous fournir, par cette voie, tous les groupes finis possibles de substitutions linéaires.

Nous nous proposons maintenant de construire effectivement ces groupes. Et, dans ce but, nous allons résoudre le problème suivant :

Étant donnée une rotation de la sphère sur elle-même, trouver la substitution linéaire correspondante.

60. Établissons d'abord des relations entre les coordonnées d'un point dans un plan et celles de sa projection stéréographique sur la sphère. Faisons passer le plan par le centre O de la sphère, et prenons ce point O comme origine des coordonnées dans le plan. Soient (ξ, η, ζ) les coordonnées des points de la sphère, les axes ξ, η étant confondus avec les axes x, y du plan.

Fig. 4.

Prenons comme centre de projection le point d'intersection V de la sphère avec la partie positive de l'axe des ζ. Soient $M(x, y)$ un point du plan; $M_1(\xi, \eta, \zeta)$ son correspondant sur la sphère; R et T les projections orthogonales de M_1 respectivement sur le plan $\xi\eta$ et l'axe ζ; N et S celles de M, R sur l'axe ξ. Les trois

points O, R, M sont évidemment en ligne droite, et l'on a

$$x = \text{ON}, \quad y = \text{NM}, \quad \xi = \text{OS}, \quad \eta = \text{SR}, \quad \zeta = \text{RM};$$

de plus, en supposant la sphère de rayon *un*,

(1) $$\xi^2 + \eta^2 + \zeta^2 = 1.$$

On voit sur la figure que

$$\frac{\text{OR}}{\text{OM}} = \frac{\text{OS}}{\text{ON}} = \frac{\text{SR}}{\text{NM}}, \qquad \frac{\text{TM}_1}{\text{OM}} = \frac{\text{TV}}{\text{OV}},$$

$$\text{TM}_1 = \text{OR}, \qquad \text{OV} = 1, \qquad \text{TV} = 1 - \text{OT} = 1 - \text{RM}_1;$$

d'où

$$\frac{\text{OS}}{\text{ON}} = \frac{\text{SR}}{\text{NM}} = \frac{1 - \text{RM}_1}{1},$$

c'est-à-dire

$$\frac{\xi}{x} = \frac{\eta}{y} = \frac{1-\zeta}{1}$$

ou

(2) $$x = \frac{\xi}{1-\zeta}, \qquad y = \frac{\eta}{1-\zeta};$$

d'où il suit, en tenant compte de (1),

$$x^2 + y^2 = \frac{\xi^2+\eta^2}{(1-\zeta)^2} = \frac{1-\zeta^2}{(1-\zeta)^2} = \frac{1+\zeta}{1-\zeta},$$

et enfin

(3) $$\xi = \frac{2x}{x^2+y^2+1}, \qquad \eta = \frac{2y}{x^2+y^2+1}, \qquad \zeta = \frac{x^2+y^2-1}{x^2+y^2+1}.$$

Les formules (2) et (3) donnent les relations cherchées.

61. Revenons à la figure 2 (n° 49); prenons C comme origine des coordonnées et supposons pour simplifier la sphère de rayon 1.

Posons

$$p = \rho e^{i\mu}, \qquad q = \rho' e^{i\mu'}.$$

L'angle PVQ étant droit et le point C étant situé sur la droite PQ entre P et Q, on aura

$$\rho\rho' = 1, \qquad \mu' = \mu + \pi;$$

d'où

$$q = -\frac{1}{\rho} e^{i\mu}.$$

Maintenant, des formules

$$\frac{z'-p}{z'-q} = \theta\,\frac{z-p}{z-q} = e^{i\alpha}\,\frac{z-p}{z-q},$$

où α est l'amplitude de la rotation, on tire

$$z' = \frac{(\theta q - p)z + pq(1-\theta)}{(\theta - 1)z + q - \theta p},$$

ou, en posant $\alpha = 2\beta$, $e^{i\beta} = \gamma$, et observant que $\frac{p}{q} = -\rho^2$,

$$(1) \qquad z' = \frac{\left(\gamma + \frac{1}{\gamma}\rho^2\right)z + p\left(\frac{1}{\gamma} - \gamma\right)}{\frac{1}{q}\left(\gamma - \frac{1}{\gamma}\right)z + \frac{1}{\gamma} + \gamma\rho^2}.$$

Or, puisque γ et $\frac{1}{\gamma}$ d'une part, p et $-\frac{1}{q}$ d'autre part sont des couples de quantités conjuguées, il en est de même des couples

$$\gamma + \frac{1}{\gamma}\rho^2, \quad \frac{1}{\gamma} + \gamma\rho^2 \qquad \text{et} \qquad p\left(\frac{1}{\gamma} - \gamma\right), \quad -\frac{1}{q}\left(\gamma - \frac{1}{\gamma}\right).$$

Donc, A, B, C, D désignant quatre quantités réelles, on pourra poser

$$\gamma + \frac{1}{\gamma}\rho^2 = D + iC, \qquad \frac{1}{\gamma} + \gamma\rho^2 = D - iC,$$

$$\frac{1}{q}\left(\gamma - \frac{1}{\gamma}\right) = B + iA, \qquad -p\left(\frac{1}{\gamma} - \gamma\right) = B - iA.$$

La substitution (1) deviendra alors

$$z' = \frac{(D + iC)z - (B - iA)}{(B + iA)z + D - iC}$$

et aura pour déterminant

$$\Delta = A^2 + B^2 + C^2 + D^2 = (\rho^2 + 1)^2.$$

Pour ramener cette substitution à la forme unitaire, il suffit de

diviser tous ses coefficients par $\rho^2 + 1$ et de poser

$$(2)\quad \left\{\begin{aligned} &\frac{1}{\rho^2+1}\left(\gamma + \frac{1}{\gamma}\rho^2\right) = d + ic,\\ &\frac{1}{\rho^2+1}\left(\frac{1}{\gamma} + \gamma\rho^2\right) = d - ic,\\ &\frac{1}{\rho^2+1}\,\frac{1}{q}\left(\gamma - \frac{1}{\gamma}\right) = b + ia,\\ -&\frac{p}{\rho^2+1}\left(\frac{1}{\gamma} - \gamma\right) = b - ia; \end{aligned}\right.$$

la substitution devient

$$(3)\qquad z' = \frac{(d+ic)z - (b-ia)}{(b+ia)z + d - ic},$$

son déterminant est égal à 1 et les quantités réelles a, b, c, d sont liées par la relation

$$(4)\qquad a^2 + b^2 + c^2 + d^2 = 1.$$

Prenons les mêmes axes ξ, η, ζ que dans le numéro précédent et définissons chaque point de la sphère à l'aide de sa longitude et de sa latitude, le plan $\xi\eta$ étant l'équateur et le plan $\xi\zeta$ le méridien origine; choisissons comme sens positifs pour la latitude et la longitude ceux qui correspondent à une rotation de $\frac{\pi}{2}$ amenant le demi-axe positif ξ respectivement en coïncidence avec les axes ζ et η.

Il existe une relation simple entre la longueur du rayon $OM = \rho$ et la latitude $MOM_1 = \lambda$ de sa projection M_1; on a (voir *fig.* 4)

$$M_1OV = \frac{\pi}{2} - \lambda$$

et, puisque le triangle M_1OV est isoscèle,

$$OVM_1 = \frac{\pi}{4} + \frac{\lambda}{2},$$

et enfin, en tenant compte de ce que $OV = 1$,

$$\rho = \operatorname{tang}\left(\frac{\pi}{4} + \frac{\lambda}{2}\right) = \frac{1 + \operatorname{tang}\frac{\lambda}{2}}{1 - \operatorname{tang}\frac{\lambda}{2}};$$

d'où

$$\operatorname{tang}\frac{\lambda}{2} = \frac{\rho - 1}{\rho + 1},$$

et, par suite,

$$(5) \qquad \sin\lambda = \frac{\rho^2 - 1}{\rho^2 + 1}, \qquad \cos\lambda = \frac{2\rho}{\rho^2 + 1}.$$

Donc, si l'on donne à ρ la même signification qu'au commencement de ce paragraphe, les relations (5) déterminent la latitude du point M_1. Nous désignerons sa longitude par μ.

Les formules (2) vont nous permettre de résoudre maintenant le problème que nous nous sommes proposé au n° 59.

Une rotation est définie si l'on connaît, outre son amplitude $\alpha = 2\beta$, la latitude λ et la longitude μ d'un de ses pôles. Or, des relations (2) on déduit, en tenant compte de (5),

$$d = \frac{1}{2}\left(\gamma + \frac{1}{\gamma}\right) = \frac{1}{2}(e^{i\beta} + e^{-i\beta}) = \cos\beta,$$

$$c = \frac{1}{2i(\rho^2+1)}\left(\gamma - \frac{1}{\gamma}\right)(1-\rho^2) = -\frac{\rho^2-1}{\rho^2+1}\,\frac{e^{i\beta}-e^{-i\beta}}{2i} = -\sin\lambda\sin\beta,$$

$$b = \frac{1}{2(\rho^2+1)}\left(\gamma - \frac{1}{\gamma}\right)\left(\frac{1}{q} + p\right) = \frac{1}{2(\rho^2+1)}(e^{i\beta} - e^{-i\beta})\rho(e^{-i\mu} + e^{i\mu})$$

$$= -\frac{2\rho}{\rho^2+1}\,\frac{e^{i\beta}-e^{-i\beta}}{2i}\,\frac{e^{i\mu}-e^{-i\mu}}{2i} = -\cos\lambda\sin\beta\sin\mu,$$

$$a = \frac{1}{2i(\rho^2+1)}\left(\gamma - \frac{1}{\gamma}\right)\left(\frac{1}{q} - p\right) = \frac{-1}{2i(\rho^2+1)}(e^{i\beta} - e^{-i\beta})\rho(e^{-i\mu} + e^{i\mu})$$

$$= \frac{-2\rho}{\rho^2+1}\,\frac{e^{i\beta}-e^{-i\beta}}{2i}\,\frac{e^{i\mu}+e^{-i\mu}}{2} = -\cos\lambda\sin\beta\cos\mu.$$

Les formules

$$(6) \qquad \begin{cases} a = -\cos\lambda\sin\beta\cos\mu, \\ b = -\cos\lambda\sin\beta\sin\mu, \\ c = -\sin\lambda\sin\beta, \\ d = \cos\beta \end{cases}$$

donnent la substitution (3) correspondant à une rotation donnée.

62. Appliquons ces résultats aux groupes finis de rotations.

Groupes cycliques. — Soit un groupe cyclique d'ordre n, ayant pour pôles les points $(0, 0, \pm 1)$.

Ici $\lambda = \frac{\pi}{2}$, μ est indéterminé; de plus,

$$\beta = \frac{1}{2}\frac{2k\pi}{n} = \frac{k\pi}{n} \qquad (k = 0, 1, 2, \ldots, n-1);$$

d'où

$$a = b = 0, \qquad c = \sin\frac{k\pi}{n}, \qquad d = \cos\frac{k\pi}{n}$$

et, par suite,

$$z' = \frac{\left(\cos\frac{k\pi}{n} + i\sin\frac{k\pi}{n}\right)z}{\cos\frac{k\pi}{n} - i\sin\frac{k\pi}{n}},$$

ou plus simplement

$$z' = e^{\frac{2k\pi i}{n}} z \qquad (k = 0, 1, 2, \ldots, n-1).$$

Groupes diédriques. — Supposons que le polygone constituant le dièdre soit situé dans le plan $\xi\eta$ et que l'un de ses sommets coïncide avec le point $(1, 0, 0)$. Le groupe comprend alors un sous-groupe cyclique d'ordre m, ayant pour pôles les points $(0, 0, \pm 1)$ et m rotations d'amplitude π autour de m droites formant entre elles des angles égaux, dont l'une coïncide avec l'axe des ξ, et qui ne sont autres que les m axes de symétrie du polygone.

Les m premières rotations correspondent aux substitutions

$$z' = e^{\frac{2k\pi i}{n}} z \qquad (k = 0, 1, 2, \ldots, m-1).$$

Pour les m autres rotations, on a

$$\lambda = 0, \qquad \beta = \frac{\pi}{2}, \qquad \mu = \frac{k\pi}{m} \qquad (k = 0, 1, 2, \ldots, m-1);$$

d'où

$$a = \cos\frac{k\pi}{m}, \qquad b = \sin\frac{k\pi}{m}, \qquad c = 0, \qquad d = 0$$

et, par suite,

$$z' = -\frac{\sin\frac{k\pi}{m} - i\cos\frac{k\pi}{m}}{\left(\sin\frac{k\pi}{m} + i\cos\frac{k\pi}{m}\right)z},$$

ou plus simplement

$$z' = \frac{e^{\frac{2k\pi i}{m}}}{z} \qquad (k = 0, 1, 2, \ldots, m-1).$$

Les substitutions du groupe diédrique sont donc données par les formules

$$(1) \qquad z' = e^{\frac{2k\pi i}{m}} z, \qquad z' = \frac{e^{\frac{2k\pi i}{m}}}{z} \qquad (k = 0, 1, 2, \ldots, m-1).$$

En particulier, les substitutions du groupe trirectangle (n° 53) sont

$$(2) \qquad z' = z, \qquad z' = -z, \qquad z' = \frac{1}{z}, \qquad z' = -\frac{1}{z}.$$

Si T désigne la substitution $z' = e^{\frac{2k\pi i}{m}} z$ correspondant à la rotation $\frac{2\pi}{m}$ autour de l'axe ζ et U la substitution $z' = \frac{1}{z}$, correspondant à la rotation π autour de l'axe ξ, toutes les substitutions du groupe seront données par

$$T^k, \qquad T^k U \qquad (k = 0, 1, 2, \ldots, m-1).$$

63. *Groupe tétraédrique.* — Disposons le tétraèdre de façon que les trois médianes coïncident avec les trois axes de coordonnées. Pour cela, imaginons qu'on inscrive dans la sphère un cube dont les faces soient parallèles aux plans de coordonnées; soient A, B, C, D quatre sommets du cube qui ne soient pas contigus deux à deux; A′, B′, C′, D′ les sommets qui leur sont respectivement opposés. Les deux tétraèdres ABCD, A′B′C′D′ sont réguliers, ont pour médianes communes les trois axes des coordonnées et sont conjugués l'un de l'autre.

Le groupe tétraédrique, nous l'avons vu (n° 54), comprend un sous-groupe trirectangle que nous représenterons par

$$(1) \qquad 1, \quad T, \quad U, \quad TU,$$

T et U étant deux rotations [1] d'amplitude π autour des axes ζ

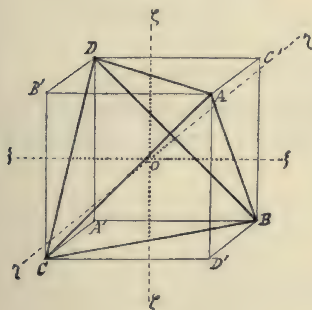
---

[1] Pour plus de simplicité, nous employons toujours la même notation pour une rotation et la substitution correspondante.

et ξ, et TU étant par conséquent une rotation d'amplitude π autour de l'axe η. L'effet de ces rotations sur l'échange des sommets peut être indiqué de la façon suivante :

$$(2)\quad \left\{\begin{array}{l} T = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}, \qquad U = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \\ \qquad\qquad TU = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}. \end{array}\right.$$

Fig. 5.



Soit S une rotation d'amplitude $\frac{2\pi}{3}$ ayant pour pôles A et A′,

$$S = \begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix};$$

son carré

$$S^2 = \begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$$

est une rotation d'amplitude $\frac{4\pi}{3}$, avec les mêmes pôles.

Étant donnée une rotation $\frac{2\pi}{3}$ ou $\frac{4\pi}{3}$ autour d'un autre sommet, nous allons montrer qu'elle s'obtient en multipliant S ou S^2 par une des trois rotations (2).

Soit en effet X cette rotation,

$$X = \begin{pmatrix} A & E_1 & E_2 & E_3 \\ E_2 & E_1 & E_3 & A \end{pmatrix},$$

E_1, E_2, E_3 désignant les sommets B, C, D pris dans un ordre quelconque. Posons

$$Y = \begin{pmatrix} A & E_1 & E_2 & E_3 \\ E_2 & E_3 & A & E_1 \end{pmatrix}.$$

On a

$$XY = \begin{pmatrix} A & E_1 & E_2 & E_3 \\ A & E_3 & E_1 & E_2 \end{pmatrix},$$

ou bien, puisque Y est d'ordre 2,

$$X = \begin{pmatrix} A & E_1 & E_2 & E_3 \\ A & E_3 & E_1 & E_2 \end{pmatrix} Y;$$

mais Y est l'une des rotations (2) et $\begin{pmatrix} A & E_1 & E_2 & E_3 \\ A & E_3 & E_1 & E_2 \end{pmatrix}$ représente soit S, soit S^2, d'où la proposition annoncée.

On peut donc ranger les rotations du groupe tétraédrique dans le Tableau suivant :

$$(3) \qquad \left\{ \begin{array}{cccc} 1 & T & U & TU, \\ S & ST & SU & STU, \\ S^2 & S^2T & S^2U & S^2TU. \end{array} \right.$$

Reste à trouver l'expression analytique des substitutions correspondantes.

Les substitutions (1) ont déjà été construites [n° 62, formules (2), page 74]. Déterminons la substitution S.

Les coordonnées du point A sont égales toutes trois à $\frac{1}{\sqrt{3}}$; les formules bien connues

$$\operatorname{tang}\lambda = \frac{\xi}{\sqrt{\xi^2 + \eta^2}}, \qquad \operatorname{tang}\mu = \frac{\eta}{\xi}$$

nous donnent

$$\operatorname{tang}\lambda = \frac{1}{\sqrt{2}}, \qquad \operatorname{tang}\mu = 1;$$

par conséquent

$$\sin\lambda = \frac{1}{\sqrt{3}}, \qquad \cos\lambda = \frac{\sqrt{2}}{\sqrt{3}}, \qquad \sin\mu = \cos\mu = \frac{1}{\sqrt{2}},$$

et, comme $\beta = \frac{\pi}{3}$,

$$\sin\beta = \frac{\sqrt{3}}{2}, \qquad \cos\beta = \frac{1}{2}.$$

D'autre part (n° 61) [formules (6)],

$$a = b = c = -\frac{1}{2}, \qquad d = \frac{1}{2},$$

en sorte que l'expression de S est

$$z' = \frac{\frac{1-i}{2}z - \frac{-1+i}{2}}{\frac{-1-i}{2}z + \frac{1+i}{2}},$$

ou, remarquant que

$$1 - i = -i(1+i),$$

$$z' = \frac{iz + i}{z - 1}.$$

En tenant compte de ce résultat, des formules (2) (n° 62) et des formules de multiplication (n° 20), on obtient les expressions de toutes les substitutions du groupe

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad TU = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$S = \begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix}, \qquad ST = \begin{pmatrix} i & i \\ -1 & 1 \end{pmatrix},$$

$$SU = \begin{pmatrix} 1 & -1 \\ i & i \end{pmatrix}, \qquad STU = \begin{pmatrix} -1 & 1 \\ i & i \end{pmatrix},$$

$$S^2 = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \qquad S^2T = \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix},$$

$$S^2U = \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \qquad S^2TU = \begin{pmatrix} -1 & i \\ 1 & i \end{pmatrix}.$$

Ces substitutions peuvent encore être mises sous la forme suivante, plus concise :

$$(4) \qquad z' = \delta z, \qquad z' = \frac{\delta}{z}, \qquad z' = \delta\frac{z + \varepsilon i}{z - \varepsilon i}, \qquad z' = \delta i \frac{z + \varepsilon}{z - \varepsilon},$$

où δ, ε représentent les valeurs ± 1.

Il n'est pas inutile, pour la suite, d'avoir les expressions de ces substitutions pour d'autres dispositions de tétraèdre; par exemple lorsqu'on l'a fait tourner de 45° autour de l'axe ζ, à partir de la première position.

Soient $\mathbf{x}$, $\mathbf{y}$; $\mathbf{x}'$, $\mathbf{y}'$ les coordonnées des nouvelles positions d'un point et de son transformé. On a

$$x = \frac{1}{\sqrt{2}}(\mathbf{x} - \mathbf{y}), \qquad y = \frac{1}{\sqrt{2}}(\mathbf{x} + \mathbf{y}),$$

$$x' = \frac{1}{\sqrt{2}}(\mathbf{x}' - \mathbf{y}'), \qquad y' = \frac{1}{\sqrt{2}}(\mathbf{x}' + \mathbf{y}'),$$

et, si l'on pose

$$\mathbf{x} + i\mathbf{y} = \mathbf{z}, \qquad \mathbf{x}' + i\mathbf{y}' = \mathbf{z}',$$

on obtient

$$(5) \qquad z = \frac{1+i}{\sqrt{2}}\mathbf{z}, \qquad z' = \frac{1+i}{\sqrt{2}}\mathbf{z}',$$

soit pour abréger

$$\frac{1+i}{\sqrt{2}} = \rho, \qquad \frac{1-i}{\sqrt{2}} = \rho';$$

la substitution

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}$$

devient

$$\rho \mathbf{z}' = \frac{\alpha\rho\mathbf{z} + \beta}{\gamma\rho\mathbf{z} + \delta}$$

ou

$$\mathbf{z}' = \frac{\alpha\mathbf{z} + \beta\rho'}{\gamma\rho\mathbf{z} + \delta},$$

en sorte que, dans la nouvelle disposition du polyèdre, la substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ prend la forme $\begin{pmatrix} \alpha & \beta\rho' \\ \gamma\rho & \delta \end{pmatrix}$ et, en tenant compte des relations

$$\rho^2 = -\rho'^2 = i, \qquad \rho\rho' = 1, \qquad \rho = i\rho',$$

ou pour les substitutions rangées dans le Tableau suivant,

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathrm{T} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\mathrm{U} = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}, \qquad \mathrm{TU} = \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix},$$

$$\mathrm{S} = \begin{pmatrix} \rho & 1 \\ 1 & -\rho' \end{pmatrix}, \qquad \mathrm{ST} = \begin{pmatrix} \rho & 1 \\ -1 & \rho' \end{pmatrix},$$

$$\mathrm{SU} = \begin{pmatrix} -\rho & 1 \\ 1 & \rho' \end{pmatrix}, \qquad \mathrm{STU} = \begin{pmatrix} \rho & -1 \\ 1 & \rho' \end{pmatrix},$$

$$\mathrm{S}^2 = \begin{pmatrix} \rho' & 1 \\ 1 & -\rho \end{pmatrix}, \qquad \mathrm{S}^2\mathrm{T} = \begin{pmatrix} \rho' & 1 \\ -1 & \rho \end{pmatrix},$$

$$\mathrm{S}^2\mathrm{U} = \begin{pmatrix} \rho' & -1 \\ 1 & \rho \end{pmatrix}, \qquad \mathrm{S}^2\mathrm{TU} = \begin{pmatrix} -\rho' & 1 \\ 1 & \rho \end{pmatrix}.$$

On peut, en donnant à δ, ε la même signification que plus haut, écrire ce Tableau sous la forme plus concise

$$z' = \delta z, \qquad z' = \frac{\delta i}{z},$$

$$z' = \delta \frac{\rho' z + \varepsilon}{z - \varepsilon\rho}, \qquad z' = \delta \frac{\varepsilon\rho z + 1}{z - \varepsilon\rho'}.$$

64. *Groupe octaédrique.* — Supposons l'octaèdre disposé de façon que ses diagonales soient dirigées suivant les axes de coordonnées; ce sera le polyèdre conjugué du cube précédent; les rotations qui le laissent invariable sont celles qui laissent invariable le tétraèdre ABCD ou qui le changent en son tétraèdre conjugué A'B'C'D' (*cf.* n° 54). Les premières sont les rotations (3) du paragraphe précédent; les secondes s'obtiennent en multipliant les précédentes par une des rotations qui échangent les deux tétraèdres : telle serait la rotation $\frac{\pi}{2}$ autour de l'axe ζ, rotation que nous désignerons par V.

On a donc, pour les rotations du groupe octaédrique, le Tableau

1	T	U	TU,
S	ST	SU	STU,
S^2	S^2T	S^2U	S^2TU,
V	TV	UV	TUV,
SV	STV	SUV	$STUV$,
S^2V	S^2TV	S^2UV	S^2TUV,

et, comme

$$T = V^2, \qquad TU = UT,$$

on peut encore les ranger dans le Tableau

1	S	S^2	U	SU	S^2U,
V	SV	S^2V	UV	SUV	S^2UV,
V^2	SV^2	S^2V^2	UV^2	SUV^2	S^2UV^2,
V^3	SV^3	S^2V^3	UV^3	SUV^3	S^2UV^3.

Les substitutions correspondantes s'obtiennent en ajoutant, à celles du paragraphe précédent, leur produit par V,

(V) $$z' = iz;$$

on obtient ainsi (¹)

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix}, \qquad S^2 = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix},$$

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad SU = \begin{pmatrix} 1 & -i \\ i & i \end{pmatrix}, \qquad S^2U = \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix},$$

$$V = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \qquad SV = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \qquad S^2V = \begin{pmatrix} i & 1 \\ 1 & -i \end{pmatrix},$$

$$UV = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}, \qquad SUV = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad S^2UV = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix},$$

$$V^2 = T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$SV^2 = ST = \begin{pmatrix} i & i \\ -1 & 1 \end{pmatrix},$$

$$S^2V^2 = S^2T = \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix},$$

$$UV^2 = TU = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$SUV^2 = STU = \begin{pmatrix} -1 & 1 \\ i & i \end{pmatrix},$$

$$S^2UV^2 = S^2TU = \begin{pmatrix} -1 & i \\ 1 & i \end{pmatrix},$$

$$V^3 = TV = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix},$$

$$SV^3 = STV = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$S^2V^3 = S^2TV = \begin{pmatrix} i & -1 \\ -1 & i \end{pmatrix},$$

$$UV^3 = TUV = \begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix},$$

$$SUV^3 = STUV = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

$$S^2UV^3 = S^2TUV = \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix},$$

(¹) Entre U et V existent quelques relations simples. U, UV étant d'ordre 2 et V d'ordre 4, on a

$$U^2 = 1, \qquad UVUV = 1, \qquad V^4 = 1,$$

d'où

$$UVU = V^3$$

et, par suite,

$$VU = UV^3.$$

Il en résulte

$$V^2U = VUV^3 = UV^6 = UV^2,$$
$$V^3U = VUV^2 = UV^3 = UV.$$

Plus simplement, les substitutions du groupe peuvent être représentées par les formules (4) (nº 63), où ε prend les valeurs ± 1, et δ les valeurs ± 1, $\pm i$.

On obtient un Tableau encore plus simple, en écrivant

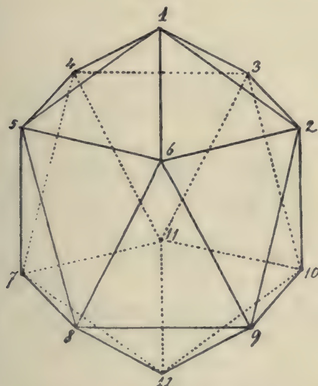
$$z' = \delta z, \qquad z' = \frac{\delta}{z}, \qquad z' = \delta \frac{z+\varepsilon}{z-\varepsilon},$$

où δ, ε peuvent prendre les valeurs ± 1, $\pm i$; on peut encore écrire

$$z' = i^h z, \qquad z' = \frac{i^h}{z}, \qquad z' = i^h \frac{z+i^k}{z-i^k} \qquad (h, k = 0, 1, 2, 3).$$

65. *Groupe icosaédrique.* — Pour plus de clarté, figurons une projection de l'icosaèdre, les sommets étant numérotés de 1 à 12.

Fig. 6.



Appelons l le côté, h la hauteur d'une face de l'icosaèdre sphérique. L'une des hauteurs partage la face en deux triangles rectangles égaux, ayant pour hypoténuse l et pour côtés de l'angle droit h, $\frac{l}{2}$; en sorte qu'on a, d'après une formule connue de trigonométrie sphérique,

$$\cos l = \cos \frac{l}{2} \cos h.$$

D'autre part, le demi-grand cercle passant par les sommets 1, 2,

12 se compose d'un côté et de deux hauteurs, d'où

$$l + 2h = \pi,$$

ou bien

$$h = \frac{\pi}{2} - \frac{l}{2}.$$

La formule précédente devient alors

$$\cos l = \cos\frac{l}{2}\sin\frac{l}{2} = \frac{1}{2}\sin l$$

ou

$$\tang l = 2;$$

d'où l'on déduit

$$\sin l = \frac{2}{\sqrt{5}}, \qquad \cos l = \frac{1}{\sqrt{5}}.$$

Il convient, pour la suite, de connaître les lignes trigonométriques de l'arc $\frac{l}{2}$. Posons $\sqrt{5} = r$; on aura

$$\sin\frac{l}{2} = \sqrt{\frac{r-1}{2r}}, \qquad \cos\frac{l}{2} = \sqrt{\frac{r+1}{2r}}.$$

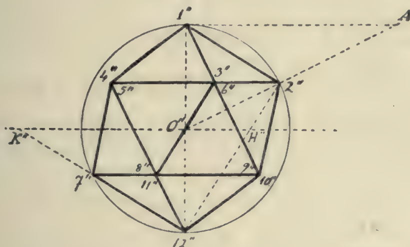
Pour l'instant montrons que l'expression trouvée pour $\tang l$ permet de donner facilement une représentation de l'icosaèdre par la méthode de Monge.

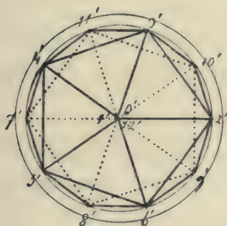
Disposons l'icosaèdre de façon que la diagonale (1 — 12) coïncide avec l'axe ζ et le plan (1.2.12) avec le plan $\xi\zeta$. Sur la figure, les lettres et les chiffres sont affectés d'un ou de deux accents suivant qu'il s'agit de projections horizontales ou de projections verticales. Prenons sur la tangente en $1''$ au contour apparent de la sphère une longueur $1''A$ égale au diamètre; la droite $O''A$, joignant A à la projection O'' du centre, rencontrera le contour apparent au point $2''$. Soit $2'$ l'autre projection du sommet 2; on inscrira dans le cercle de centre O' passant par $2'$ un pentagone régulier, ayant pour sommets $2'$, $3'$, $4'$, $5'$, $6'$.

Les points confondus $3''$ et $6''$ de même que $4''$, $5''$ sont situés sur la parallèle à la ligne de terre menée par $2''$. Les points $7'$, $8'$, $9'$, $10'$, $11'$ sont diamétralement opposés sur le cercle O' respectivement à $2'$, $3'$, $4'$, $5'$, $6'$. Les projections verticales correspondantes se trouvent sur une parallèle à la ligne de terre symétrique de la

précédente par rapport à O″. Comme vérification, on peut observer que, le point 2 étant dans le plan $\xi\zeta$, les sommets adjacents 1, 3, 10, 9, 6 se trouvent dans un plan perpendiculaire au précédent et que

Fig. 7.





par conséquent leurs projections verticales sont en ligne droite ; on peut en dire autant des points 4, 5, 8, 12, 11.

66. Il convient ici de faire une remarque, qui nous sera utile dans un instant.

Étant données deux rotations P_1, P_2 d'amplitudes α_1, α_2 autour des axes l_1, l_2, on a identiquement

$$P_1 P_2 \equiv P_2(P_2^{-1} P_1 P_2).$$

Or (n° 31) $P_2^{-1} P_1 P_2$ est une rotation d'angle α_1 autour de l'axe l'_1, transformé de l_1 par la rotation P_2. Donc, pour obtenir la rotation $P_1 P_2$ on peut, soit effectuer successivement les rotations P_1 et P_2, soit effectuer d'abord P_2, puis une rotation P'_1 de même

angle α_1 que P_1 autour de l'axe l'_1 transformé de l_1 par la rotation P_2.

Cela posé, nous allons établir que toutes les rotations du groupe icosaédrique peuvent être composées à l'aide des trois rotations suivantes :

1° Une rotation S d'amplitude $\frac{2\pi}{3}$ autour de la diagonale (1.12);

2°. Une rotation T d'amplitude π autour de la droite joignant les milieux des arêtes (1.2), (7.12);

3° Une rotation U d'amplitude π autour de la droite joignant les milieux des arêtes (6.8), (3.11).

Soit à effectuer la rotation qui amène l'arête 1.2 en coïncidence avec une autre arête quelconque $\mu\nu$. Nous distinguerons trois cas :

a. μ est le sommet 1; alors la rotation considérée est S ou une de ses puissances.

b. μ est un des sommets 2, 3, 4, 5, 6. Pour amener le sommet 1 en μ, on effectuera d'abord la rotation T amenant 1 en 2, puis, si μ est différent de 2, la rotation $S^{\mu-2}$ qui amène 1 en μ [1].

Si, après ces deux opérations, 2 ne coïncide pas avec ν, on pourra obtenir ce résultat au moyen d'une rotation autour de μ, ayant pour amplitude un multiple de $\frac{2\pi}{5}$. Posons

$$N = TS^{\mu-2};$$

M est (n° 31) la transformée par N d'une rotation d'angle égal, dont l'un des pôles est 1, c'est-à-dire d'une rotation S^λ, λ étant l'un des nombres 0, 1, 2, 3, 4 (l'hypothèse $\lambda = 0$ correspondrait au cas où ν coïnciderait déjà avec 2). Donc, en tenant compte d'une remarque faite un peu plus haut,

$$NM = S^\lambda N = S^\lambda TS^{\mu-2}.$$

La rotation considérée est donc composée à l'aide des rotations S et T et de la façon indiquée par cette dernière formule.

c. μ est un des six autres sommets. Si l'arête $\mu\nu$ par l'effet de la rotation U se transforme en $\mu'\nu'$, μ' sera un des sommets 1, 2, 3, 4,

(1) Il ne faut pas oublier que les axes de rotation doivent être considérés comme fixes dans l'espace. Pour bien faire comprendre ce qui précède, imaginons un icosaèdre fixe et un autre mobile, coïncidant primitivement avec le premier. Lorsqu'on dit qu'une rotation amène l'arête $\alpha\beta$ sur l'arête $\gamma\delta$, il faut entendre par là que cette rotation appliquée à l'icosaèdre mobile amène l'arête $\alpha\beta$ de ce dernier à coïncider avec l'arête $\gamma\delta$ de l'icosaèdre fixe.

5, 6 et l'on pourra faire coïncider 1.2 avec $\mu'\nu'$ à l'aide d'une transformation du type S^h ou S^hTS^k. Il en résulte qu'on fera coïncider 1.2 avec $\mu\nu$ à l'aide d'une transformation de l'un des deux types S^hU, S^hTS^kU.

En résumé : *Toutes les rotations du groupe icosaédrique s'expriment à l'aide des trois rotations* S, T, U *et appartiennent aux quatre types suivants :*

$$S^\lambda,\quad S^hTS^k,\quad S^hU,\quad S^\lambda TS^kU \qquad (h, k = 0, 1, 2, 3, 4).$$

On vérifie de suite que les rotations correspondantes sont au nombre de 60 ; c'est précisément le nombre des rotations du groupe icosaédrique.

Ajoutons que U peut s'exprimer à l'aide de S et T.

En effet, d'après ce qui précède, S^2TS^3 amène le sommet 1 en 5. Pour voir ce que devient en même temps le sommet 2, observons que, T amenant 1.2 en 2.1, TS^3 amène 1.2 en 5.1 et qu'une multiplication à gauche par S^2 équivaut à une rotation $\frac{4\pi}{5}$ autour du sommet 5, rotation qui amène 5.1 en 5.7. Donc S^2TS^3 amène 1.2 en 5.7.

D'autre part, TS^2T, étant la transformée de S^2 par T, représente une rotation $\frac{4\pi}{5}$ autour de l'axe 2.7, et amène par suite 5.7 en 12.7.

Donc la rotation $S^2TS^3TS^2T$ amène 1.2 en 12.7. C'est là précisément l'effet de la rotation U, d'où

$$S^2TS^3TS^2T = U.$$

67. Les rotations 1, T, U, TU forment un groupe trirectangle, qui est un sous-groupe du groupe tétraédrique ; les axes des trois rotations T, U, TU sont trois médianes, orthogonales deux à deux ([1]).

Il est évident, par raison de symétrie, qu'il existe cinq systèmes orthogonaux de ce genre, qu'on déduit de l'un quelconque d'entre eux en le faisant tourner autour de l'axe ζ de l'angle $\frac{2\pi}{5}$ et de

([1]) Il est facile du reste de trouver directement ces médianes sur la figure 7. En adoptant pour ces médianes la même notation que dans le texte, on voit que les médianes (1.2 — 7.12), (4.5 — 9.10) sont situées dans le plan $\xi\zeta$; que leurs projections sont 3″.11″, 4″.10″ ; que ces projections sont perpendiculaires comme diagonales d'un losange. De plus, la médiane (3.11 — 6.8) a même direction que l'axe η et est, par conséquent, perpendiculaire aux deux autres.

ses multiples. Les quinze médianes de l'icosaèdre se partagent en cinq systèmes de trois droites orthogonales disposées symétriquement autour d'une diagonale quelconque.

Désignons par k_1, k_2, k_3, k_4, k_5 ces cinq systèmes de médianes. Toute rotation du groupe icosaédrique laisse chaque système invariable ou le change en un autre, en sorte qu'aux soixante rotations du groupe correspondent soixante permutations des cinq systèmes.

Montrons que ces permutations sont l'ensemble des permutations paires de cinq éléments.

Désignons en général par $(\alpha\beta - \gamma\delta)$ la médiane passant par les milieux des arêtes $\alpha\beta$ et $\gamma\delta$. Nous aurons

$$\begin{array}{lll} k_1 = (1.2 - 7.12), & (3.11 - 6.8), & (4.5 - 9.10), \\ k_2 = (1.3 - 8.12), & (4.7 - 2.9), & (5.6 - 10.11), \\ k_3 = (1.4 - 9.12), & (5.8 - 3.10), & (6.2 - 11.7), \\ k_4 = (1.5 - 10.12), & (6.9 - 4.11), & (2.3 - 7.8), \\ k_5 = (1.6 - 11.12), & (2.10 - 5.7), & (3.4 - 8.9). \end{array}$$

L'effet des rotations S, T, U sur les sommets et sur les médianes est résumé dans le Tableau suivant :

I.	S.	T.	U.
1	1	2	12
2	3	1	7
3	4	6	11
4	5	9	10
5	6	10	9
6	2	3	8
7	8	12	2
8	9	11	6
9	10	4	5
10	11	5	4
11	7	8	3
12	12	7	1
k_1	k_2	k_1	k_1
k_2	k_3	k_3	k_5
k_3	k_4	k_2	k_4
k_4	k_5	k_5	k_3
k_5	k_1	k_4	k_2

On voit donc bien que les permutations subies par les k, quand on applique les rotations S, T, U, sont paires. On peut en dire autant de la permutation correspondant à chaque rotation du groupe icosaédrique, puisque toutes ces rotations s'expriment par des produits de S, T, U; et puisque à des rotations différentes correspondent des permutations différentes ([1]) et que les rotations du groupe icosaédrique sont précisément en nombre égal à celui des permutations paires de cinq éléments, notre proposition est démontrée.

Voyons combien il y a de rotations du groupe icosaédrique, changeant en lui-même un système donné, k_1 par exemple. Les intersections de la sphère avec les trois médianes du système k_1 sont les sommets d'un octaèdre régulier h_1, et, si k_1 reste inaltéré par une rotation de la sphère, il en est de même de l'octaèdre : cette rotation appartient donc au groupe octaédrique correspondant. Et comme de telles rotations forment évidemment un groupe (qui est un sous-groupe du groupe icosaédrique), ce groupe coïncide soit avec le groupe de l'octaèdre h_1, soit avec un de ses sous-groupes. Déterminons l'ordre de ce groupe.

Un des sommets de h_1 peut être amené à coïncider soit avec lui-même, soit avec un des cinq autres, et, dans ces conditions, l'arête (de l'icosaèdre sphérique), dont il est le milieu, peut coïncider avec l'arête ayant pour milieu l'autre sommet, et cela de deux façons différentes. Chaque coïncidence peut être réalisée avec une seule rotation du groupe icosaédrique (n° 51). Il suit de là que le sous-groupe considéré comprend douze rotations. Mais le seul sous-groupe d'ordre 12 d'un groupe octaédrique est un groupe tétraédrique (n° 54); donc, *l'ensemble des rotations du groupe icosaédrique, qui laissent invariable un système de trois médianes orthogonales, constitue un groupe tétraédrique.*

Soient Γ_1, Γ_2, Γ_3, Γ_4, Γ_5 les sous-groupes tétraédriques laissant respectivement invariables les systèmes k_1, k_2, k_3, k_4, k_5. Les pôles des rotations de Γ_2, Γ_3, Γ_4, Γ_5 s'obtiennent en appliquant aux pôles de Γ_1 les rotations S, S^2, S^3, S^4; d'où il

---

([1]) S'il en était autrement, il existerait une rotation non nulle laissant inaltérés tous les systèmes de trois médianes, ce qui est impossible comme il est facile de s'en rendre compte.

suit (n° 31)

$$\Gamma_2 = S^{-1}\Gamma_1 S, \qquad \Gamma_3 = S^{-2}\Gamma_1 S^2, \qquad \Gamma_4 = S^{-3}\Gamma_1 S^3, \qquad \Gamma_5 = S^{-4}\Gamma_1 S^4.$$

68. Établissons maintenant l'expression analytique des substitutions correspondant aux rotations S, T, U.

L'expression de S est (n° 62)

$$z' = e^{\frac{2\pi i}{5}} z.$$

U est la même rotation que celle qu'on avait désignée (n°s 63 et 64) par TU; elle a pour expression

$$z' = -\frac{1}{z}.$$

Formons T, on a ici

$$\lambda = \frac{\pi}{2} - \frac{l}{2}, \qquad \mu = 0, \qquad \beta = \frac{\pi}{2};$$

d'où

$$a = -\sin\frac{l}{2}, \qquad b = 0, \qquad c = -\cos\frac{l}{2}, \qquad d = 0,$$

c'est-à-dire (n° 65)

$$a = -\sqrt{\frac{r-1}{2r}}, \qquad b = 0, \qquad c = -\sqrt{\frac{r+1}{2r}}, \qquad d = 0 \qquad (r = \sqrt{5}),$$

en sorte que la substitution cherchée est

$$z' = \frac{\sqrt{r+1}\,z + \sqrt{r-1}}{\sqrt{r-1}\,z - \sqrt{r+1}}$$

ou bien

$$z' = \frac{(r+1)z + 2}{2z - (r+1)}.$$

L'expression de cette substitution se simplifie si l'on y introduit le symbole

$$\varepsilon = e^{\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}.$$

Calculons $\sin\frac{2\pi}{5}$ et $\cos\frac{2\pi}{5}$. Dans le triangle sphérique rectangle considéré au commencement du n° 65 l'angle formé par les côtés $\frac{l}{2}$

et l est égal à $\frac{2\pi}{5}$, d'où, par une formule connue de trigonométrie sphérique,

$$\cos\frac{2\pi}{5} = \frac{\operatorname{tang}\frac{l}{2}}{\operatorname{tang} l},$$

c'est-à-dire (n° 65)

$$\cos\frac{2\pi}{5} = \frac{1}{2}\sqrt{\frac{r-1}{r+1}} = \frac{r-1}{4} = \frac{1}{r+1};$$

d'où, en tenant compte de ce que $(r+1)^2 = 6+2r$,

$$\sin\frac{2\pi}{5} = \sqrt{1-\frac{r-1}{4(r+1)}} = \frac{1}{2}\sqrt{\frac{3r+5}{r+1}}$$
$$= \frac{1}{2}\sqrt{\frac{r(6+2r)}{2(r+1)}} = \frac{1}{4}\sqrt{2r(r+1)} \quad (^1).$$

Il suit de là

$$\varepsilon = \frac{1}{4}\left[r-1+i\sqrt{2r(r+1)}\right],$$

et, comme d'après une propriété connue des racines de l'unité ε et ε^4 sont des quantités conjuguées, on a

$$\varepsilon^4 = \frac{1}{4}\left[r-1-i\sqrt{2r(r+1)}\right].$$

De plus,

$$\varepsilon^2+\varepsilon^3 = -1-(\varepsilon+\varepsilon^4) = -1-\frac{1}{2}(r-1) = -\frac{1}{2}(r+1),$$

$$\varepsilon^2-\varepsilon^3 = \varepsilon^2-\varepsilon^8 = (\varepsilon+\varepsilon^4)(\varepsilon-\varepsilon^4)$$
$$= \frac{1}{2}(r-1)\frac{1}{2}i\sqrt{2r(r+1)}$$
$$= \frac{1}{4}i(r-1)\sqrt{2r(r+1)}$$
$$= \frac{1}{2}i\sqrt{2r(r-1)};$$

---

(1) Ces expressions conduisent aux formules

$$\sin\frac{\pi}{5} = \frac{1}{4}\sqrt{2r(r-1)}, \qquad \cos\frac{\pi}{5} = \frac{r+1}{4},$$

qui nous serviront dans la suite.

d'où

$$\varepsilon^2 = \frac{1}{4}\left[-(r+1) + i\sqrt{2r(r-1)}\right],$$

$$\varepsilon^3 = \frac{1}{4}\left[-(r+1) - i\sqrt{2r(r-1)}\right].$$

Posons

$$\sigma = \varepsilon - \varepsilon^4 = \frac{1}{2} i\sqrt{2r(r+1)},$$

$$\tau = \varepsilon^2 - \varepsilon^3 = \frac{1}{2} i\sqrt{2r(r-1)};$$

σ et τ sont liés par les relations

$$\sigma\tau = -r, \qquad \sigma^2 + \tau^2 = -5, \qquad \sigma^2 - \tau^2 = -r.$$

Les substitutions T et S peuvent s'écrire

$$z' = \frac{\sigma z + \tau}{\tau z - \sigma},$$

$$z' = \varepsilon z;$$

d'où, pour la substitution S^h,

$$z' = \varepsilon^h z.$$

En partant de ces formules, on construit facilement le Tableau des substitutions du groupe icosaédrique :

$$S^h = \begin{pmatrix} \varepsilon^h & 0 \\ 0 & 1 \end{pmatrix},$$

$$S^h T S^k = \begin{pmatrix} \varepsilon^{h+k} & \varepsilon^k \tau \\ \varepsilon^h \tau & -\sigma \end{pmatrix}, \qquad S^h U = \begin{pmatrix} 0 & 1 \\ -\varepsilon^h & 0 \end{pmatrix},$$

$$S^h T S^k U = \begin{pmatrix} -\varepsilon^h \tau & \sigma \\ \varepsilon^{h+k}\sigma & \varepsilon^h \tau \end{pmatrix} \text{ [1]}.$$

Il convient, pour la suite, de mettre ces substitutions sous forme de substitutions unitaires. Il suffit, pour cela, de diviser les éléments de chacune d'elles par la racine carrée de son déterminant.

---

[1] Ces substitutions ne sont pas toutes identiques à celles du groupe icosaédrique données par M. Klein. On passe des unes aux autres au moyen du changement de variables

$$z_1 = -z, \qquad z'_1 = -z'.$$

On obtient ainsi

$$S^h = \begin{pmatrix} \varepsilon^{\frac{h}{2}} & 0 \\ 0 & \varepsilon^{-\frac{h}{2}} \end{pmatrix},$$

$$S^h T S^k = \begin{pmatrix} \frac{1}{r} e^{\frac{1}{2}(h+k)}\sigma & \frac{1}{r} e^{\frac{1}{2}(-h+k)}\tau \\ \frac{1}{r} e^{\frac{1}{2}(h-k)}\tau & -\frac{1}{r} e^{-\frac{1}{2}(h+k)}\sigma \end{pmatrix},$$

$$S^h U = \begin{pmatrix} 0 & \varepsilon^{-\frac{h}{2}} \\ -\varepsilon^{\frac{h}{2}} & 0 \end{pmatrix},$$

$$S^h T S^k U = \begin{pmatrix} -\frac{1}{r} e^{\frac{1}{2}(h-k)}\tau & \frac{1}{r} e^{-\frac{1}{2}(h+k)}\sigma \\ \frac{1}{r} e^{\frac{1}{2}(h+k)}\sigma & \frac{1}{r} e^{\frac{1}{2}(-h+k)}\tau \end{pmatrix}.$$

69. Nous savons que les substitutions du groupe icosaédrique sont d'ordres 2, 3, 5. Voyons comment on peut reconnaître directement l'ordre d'une substitution de ce groupe.

Rappelons que, si une substitution est mise sous la forme unitaire (3) (n° **61**), on a

$$d = \cos\beta,$$

β désignant la demi-amplitude de la rotation correspondante; de plus, d est la demi-somme des termes extrêmes de la substitution. On a donc :

Pour S^h,

$$(1)\qquad \cos\beta = \frac{1}{2}\left(\varepsilon^{\frac{h}{2}} + \varepsilon^{-\frac{h}{2}}\right) = \cos\frac{h\pi}{5};$$

pour $S^h T S^k$,

$$(2)\qquad \cos\beta = \frac{\sigma}{2r}\left(\varepsilon^{\frac{1}{2}(h+k)} - \varepsilon^{-\frac{1}{2}(h+k)}\right) = -\frac{\sigma}{ri}\sin\frac{h+k}{5}\pi;$$

pour $S^h U$,

$$(3)\qquad \cos\beta = 0;$$

pour $S^h T S^k U$,

$$(4)\qquad \cos\beta = \frac{\tau}{2r}\left(\varepsilon^{\frac{1}{2}(-h+k)} - \varepsilon^{\frac{1}{2}(h-k)}\right) = \frac{\tau}{ri}\sin\frac{h-k}{5}\pi.$$

On voit, d'après (1), que les substitutions $S^h (h = 1, 2, 3, 4)$ sont d'ordre 5, et d'après (3) que les substitutions

$$S^h U \qquad (h = 0, 1, 2, 3, 4)$$

sont d'ordre 2.

Cherchons maintenant quelles sont les substitutions $S^h T S^k$, d'ordre 2. On doit avoir

$$\beta = \frac{\pi}{2},$$

par suite

$$\sin \frac{h+k}{5} \pi = 0;$$

d'où

$$h + k \equiv 0 \pmod 5.$$

En second lieu, cherchons quelles sont les substitutions $S^h T S^k$, d'ordre 3. On doit avoir, soit

$$\beta = \frac{\pi}{3},$$

soit

$$\beta = \frac{2\pi}{3};$$

par suite

$$\cos \beta = \pm \frac{1}{2}$$

et

$$\sin \frac{h+k}{5} \pi = \mp \frac{ri}{2\sigma} = \mp \frac{r}{\sqrt{2r(r+1)}} = \mp \frac{1}{4} \sqrt{2r(r-1)},$$

d'où (*voir* note, p. 89)

$$\sin \frac{h+k}{5} \pi = \mp \sin \frac{\pi}{5}$$

et, par suite,

$$h + k \equiv \mp 1 \pmod 5.$$

Les substitutions restantes $S^h T S^k$, pour lesquelles on a

$$h + k \equiv \mp 2 \pmod 5,$$

sont nécessairement d'ordre 5.

Opérons de même pour les substitutions $S^h T S^k U$; nous trouvons :

Pour l'ordre 2,

$$\sin \frac{h-k}{5} \pi = 0, \qquad h - k \equiv 0 \pmod 5;$$

pour l'ordre 3,

$$\sin\frac{h-k}{5}\pi = \pm\frac{ri}{2\pi} = \pm\frac{r}{\sqrt{2r(r-1)}} = \pm\frac{1}{4}\sqrt{2r(r+1)} = \pm\sin\frac{2\pi}{5},$$

d'où

$$h-k \equiv \pm 2 \pmod 5;$$

pour l'ordre 5,

$$h-k \equiv \pm 1 \pmod 5.$$

En résumé, le groupe icosaédrique comprend les substitutions suivantes (*cf.* n° 53) :

La substitution identique ;

Les substitutions d'ordre 2

$$S^h U \qquad (h = 0, 1, 2, 3, 4),$$

$$S^h T S^k \qquad (h, k = 0, 0;\ 1, 4;\ 2, 3;\ 3, 2;\ 4, 1),$$

$$S^h T S^k U \qquad (h, k = 0, 0;\ 1, 1;\ 2, 2;\ 3, 3;\ 4, 4);$$

Les substitutions d'ordre 3

$$S^h T S^k \qquad (h, k = 0, 1;\ 1, 0;\ 2, 4;\ 3, 3;\ 4, 2;\ 0, 4;\ 1, 3;\ 2, 2;\ 3, 1;\ 4, 0),$$

$$S^h T S^k U \qquad (h, k = 0, 3;\ 1, 4;\ 2, 0;\ 3, 1;\ 4, 2;\ 0, 2;\ 1, 3;\ 2, 4;\ 3, 0;\ 4, 1);$$

Les substitutions d'ordre 5

$$S^h \qquad (h = 1, 2, 3, 4),$$

$$S^h T S^k \qquad (h, k = 0, 2;\ 1, 1;\ 2, 0;\ 3, 4;\ 4, 3;\ 0, 3;\ 1, 2;\ 2, 1;\ 3, 0;\ 4, 4),$$

$$S^h T S^k U \qquad (h, k = 0, 4;\ 1, 0;\ 2, 1;\ 3, 2;\ 4, 3;\ 0, 1;\ 1, 2;\ 2, 3;\ 3, 4;\ 4, 0).$$

70. Tous les réseaux considérés, y compris le réseau tétraédrique, relatif au polyèdre, pris dans sa seconde position, ont pour cercle de symétrie le grand cercle intersection de la sphère et du plan $\xi\zeta$. Il suit de là que les groupes correspondants peuvent être amplifiés par la réflexion

$$z' = \bar{z}.$$

Il est inutile d'écrire les opérations de chacun des groupes amplifiés : ce sont, outre les opérations des groupes primitifs, celle qu'on en déduit en y remplaçant z par $\bar{z}$.

71. Les considérations développées au n° 38 permettent de construire immédiatement des groupes homogènes, correspondant

aux groupes non homogènes précédents. Bornons-nous à en donner la représentation analytique.

Groupes cycliques :

$$z'_1 = \pm e^{\frac{k\pi i}{n}} z_1, \qquad z'_2 = \pm e^{-\frac{k\pi i}{n}} z^2 \qquad (k = 0, 1, 2, \ldots, n-1)$$

ou encore

$$\left.\begin{array}{ll} z'_1 = e^{\frac{k\pi i}{n}} z_1, & z'_2 = e^{-\frac{k\pi i}{n}} z_2 \\ z'_1 = e^{\frac{(k+n)\pi i}{n}} z_1, & z'_2 = e^{-\frac{(k+n)\pi i}{n}} z_2 \end{array}\right\} \quad (k = 0, 1, 2, \ldots, n-1)$$

ou plus simplement

$$z'_1 = e^{\frac{k\pi i}{n}} z_1, \qquad z'_2 = e^{-\frac{k\pi i}{n}} z_2 \qquad (h = 0, 1, 2, \ldots, 2n-1).$$

Groupes diédriques. — En opérant comme plus haut, on trouve

$$\left.\begin{array}{ll} z'_1 = e^{\frac{h\pi i}{m}} z_1, & z'_2 = e^{-\frac{h\pi i}{m}} z_2 \\ z'_1 = ie^{\frac{h\pi i}{m}} z_1, & z'_2 = ie^{-\frac{h\pi i}{m}} z_2 \end{array}\right\} \quad (h = 0, 1, 2, \ldots, 2m-1).$$

Nous aurons, en particulier, pour le groupe trirectangle ($m = 2$),

$$\left.\begin{array}{ll} z'_1 = i^h z_1, & z'_2 = i^{-h} z_2 \\ z'_1 = i^{h+1} z_2, & z'_2 = i^{-h+1} z_1 = -\, i^{-(h+1)} z_1 \end{array}\right\} \quad (h = 0, 1, 2, 3).$$

Remplaçons, dans les secondes formules, $h+1$ par h; à cause de $i^4 = 1$, quand h prend les valeurs 0, 1, 2, 3, on peut donner à $h+1$ au lieu des valeurs 1, 2, 3, 4 les mêmes valeurs 0, 1, 2, 3. Alors, les substitutions du groupe trirectangle peuvent être mises sous la forme plus simple

$$\left.\begin{array}{ll} z'_1 = i^h z_1, & z'_2 = i^{-h} z_2 \\ z'_1 = i^h z_2, & z'_2 = -\, i^{-h} z_1 \end{array}\right\} \quad (h = 0, 1, 2, 3).$$

Groupe tétraédrique. — Posons

$$\alpha = \frac{1+i}{2}, \qquad \beta = \frac{1-i}{2}, \qquad \delta = \pm 1, \qquad \varepsilon = \pm 1;$$

on a

$$\left.\begin{array}{ll} z'_1 = i^h z_1, & z'_2 = i^{-h} z_2 \\ z'_1 = i^h z_2, & z'_2 = -i^{-h} z_1 \end{array}\right\} \quad (h = 0, 1, 2, 3),$$

$$\begin{array}{ll} z'_1 = \delta(\varepsilon\alpha z_1 - \beta z_2), & z'_2 = \delta(\alpha z_1 + \varepsilon\beta z_2), \\ z'_1 = \delta(\varepsilon\beta z_1 - \alpha z_2), & z'_2 = \delta(\beta z_1 + \varepsilon\alpha z_2), \\ z'_1 = \delta\beta(\varepsilon z_1 - z_2), & z'_2 = \delta\alpha(z_1 + \varepsilon z_2), \\ z'_1 = \delta\alpha(z_1 + \varepsilon z_2), & z'_2 = \delta\beta(-\varepsilon z_1 + z_2). \end{array}$$

Groupe octaédrique. — Pour obtenir les substitutions de ce groupe, il suffit de multiplier les précédentes par la substitution

$$z'_1 = \frac{1+i}{\sqrt{2}} z_1, \qquad z'_2 = \frac{1-i}{\sqrt{2}} z_2.$$

Groupe icosaédrique. — En tenant compte des égalités

$$\varepsilon^{\frac{h}{2}} = (-1)^h \varepsilon^{\frac{6h}{2}} = (-1)^h \varepsilon^{3h},$$
$$\varepsilon^{-\frac{h}{2}} = (-1)^h \varepsilon^{\frac{4h}{2}} = (-1)^h \varepsilon^{2h},$$

on obtient les substitutions suivantes :

$$\left.\begin{array}{ll} z'_1 = \pm \varepsilon^{3h} z_1, & z'_2 = \pm \varepsilon^{2h} z_2 \\ z'_1 = \pm \varepsilon^{2h} z_2, & z'_2 = \mp \varepsilon^{3h} z_1 \\ \multicolumn{2}{l}{z'_1 = \pm \frac{1}{r}(\varepsilon^{3(h+k)} \sigma z_1 + \varepsilon^{2h+3k} \tau z_2)} \\ \multicolumn{2}{l}{z'_2 = \pm \frac{1}{r}(\varepsilon^{3h+2k} \tau z_1 - \varepsilon^{2(h+k)} \sigma z_2)} \\ \multicolumn{2}{l}{z'_1 = \pm \frac{1}{r}(\varepsilon^{3h+2k} \tau z_1 - \varepsilon^{2(h+k)} \sigma z_2)} \\ \multicolumn{2}{l}{z'_2 = \mp \frac{1}{r}(\varepsilon^{3(h+k)} \sigma z_1 + \varepsilon^{2h+3k} \tau z_2)} \end{array}\right\} \quad (h, k = 0, 1, 2, 3, 4).$$

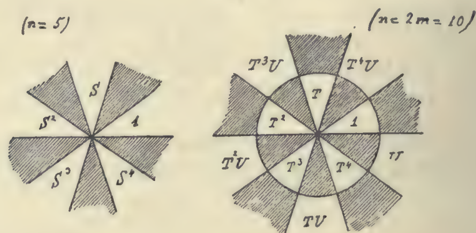
Représentation des groupes finis sur le plan.

72. Occupons-nous maintenant de la représentation plane des groupes, représentation dont nous avons dit un mot au n° 58.

Nous prendrons pour centre de la projection stéréographique le point $(0, 0, -1)$, comme plan de projection le plan $\xi\eta$, les axes x, y de ce plan coïncidant avec les axes ξ, η.

Pour les groupes cycliques et diédriques, nous nous bornerons à indiquer les figures :

Fig. 8.



Le réseau tétraédrique se compose des six grands cercles contenant les six arêtes du tétraèdre. Deux d'entre eux, contenant les arêtes AD, BC (voir *fig.* 5, p. 75), passent par le centre de projection et sont inclinés de 45° sur le plan $\xi\zeta$; ils se projettent suivant deux droites passant par l'origine et inclinées de 45° sur l'axe des x. Cherchons à obtenir la projection d'un des quatre autres cercles, par exemple du cercle contenant l'arête AC. Pour cela, représentons au moyen de la méthode de Monge la sphère et le tétraèdre inscrit : soient P et Q les intersections du plan $\xi\zeta$ avec le grand cercle passant par les points A et C, et situé dans un plan perpendiculaire. Soient L, L_1 ; M, M_1 ; N, N_1 les intersections de la sphère avec les trois axes de coordonnées; menons HN'' parallèle à la ligne de terre. Comme $P''Q''$ fait un angle de 45° avec les axes ξ et ζ, on a

$$HN''P' = P''N''L''_1 = \frac{\pi}{8},$$

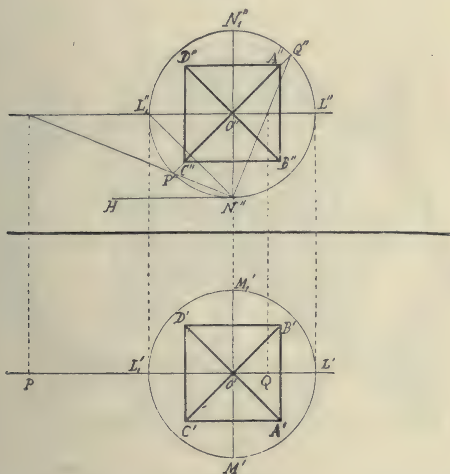
en sorte que $N''P''$ et $N''Q''$ sont les bissectrices des angles formés par les rayons $N''H$ et $N''L''_1$. Il suit de là que le faisceau

$$N''(QP''L''_1H)$$

est harmonique. Donc, si P, Q, L_1 (ou L'_1) sont les projections stéréographiques sur le plan de représentation des points désignés par les mêmes lettres, les quatre points Q, L_1, P, ∞ forment une division harmonique, et par suite L_1 est le milieu du segment PQ. Or la projection stéréographique du cercle cherché passe par P

et Q, et, comme le plan du cercle est perpendiculaire au plan $\xi\zeta$, le centre de la projection est situé sur le segment PQ; donc,

Fig. 9.



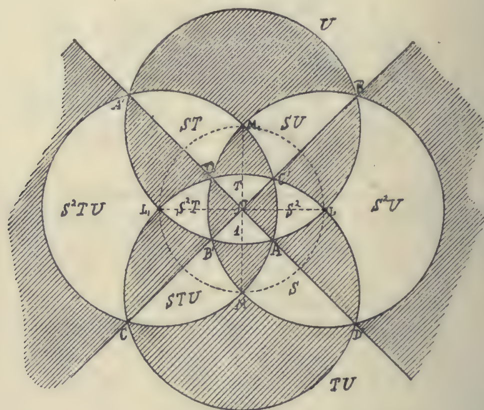
ce centre coïncide avec L_1. Il est facile de vérifier que le cercle passe nécessairement par les points M et M_1, et a un rayon égal à $\sqrt{2}$.

Dans ces conditions, pour tracer la figure cherchée, il suffit de prendre pour centre des cercles chacun des points de rencontre de l'équateur avec les axes et de faire passer le cercle par les deux points adjacents.

Les quatre cercles ainsi tracés et les deux droites précédentes partagent le plan en 24 triangles. Nous en couvrirons douze de hachures, de façon que deux triangles adjacents quelconques soient toujours l'un blanc, l'autre ombré. Choisissons comme triangle initial 1 un quelconque des triangles blancs, par exemple celui qui a un sommet à l'origine et un autre en A. Du triangle 1 on déduit le triangle T par une rotation π autour de N_1 et les triangles S, S^2 par des rotations $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ autour de A.

De S et S^2, on déduit immédiatement les triangles ST, S^2T; et enfin par une rotation π autour de l'axe des x, on obtient les triangles restants U, TU, SU, S^2U, STU, S^2TU.

Fig. 10.



73. Proposons-nous de donner une autre représentation plane des mêmes groupes en prenant comme nouveau centre de projection le centre sphérique de l'une des faces du tétraèdre, par exemple A'. Alors A se projette suivant l'origine, et les cercles ABA'B', ACA'C', ADA'D' ont pour images trois droites également inclinées, issues de A. Les points B, C, D sont situés sur ces droites et forment un triangle équilatéral de centre A. Ces points une fois marqués, et on peut prendre arbitrairement leur distance commune au point A ([1]), on trouve les autres en remarquant que C, D, B', A', sommets d'une même face du cube AB'DC'BD'CA', sont dans un même plan et, par suite, situés sur un cercle, et que l'image de B' se trouve à l'intersection des images de C et de D. Le point B' est donc l'intersection de CD avec le prolongement de BA.

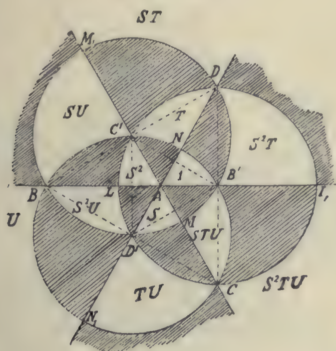
On détermine d'une façon analogue les points C' et D'. Pour achever la figure, il reste à tracer les cercles CDC'D', DBD'B',

---

([1]) Si 1 est le rayon de la sphère, on a $AB = \sqrt{2}$.

BCB′C′ et il est facile de démontrer qu'ils ont pour centres B′, C′, D′; il suffit d'observer que le triangle BC′D′ et les analogues sont équilatéraux.

Fig. 11.



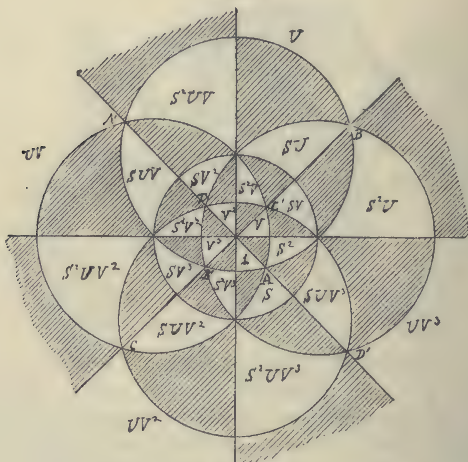
74. Dans la figure 10 se trouve déjà dessiné le cube (sphérique) AB′DC′BD′CA′; les cercles de symétrie sont les mêmes que ceux de l'octaèdre, ayant pour diagonales les axes de coordonnées. Pour avoir le réseau octaédrique, on complétera la figure 10 en y introduisant les cercles de symétrie qui y manquent, c'est-à-dire les cercles contenant les médianes des différentes faces du cube. Ces cercles, qui sont les sections de la sphère par les plans de coordonnées, ont pour projections les deux axes et le cercle équatorial.

Prenons comme triangle initial 1 le triangle ayant deux de ses sommets l'un à l'origine, l'autre au point A. Les autres triangles se croisant à l'origine auront pour symboles V, V^2, V^3, tandis que ceux qui ont leurs sommets en A auront pour symboles S, S^2. Par des rotations $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ autour de l'origine, les triangles S, S^2 deviennent respectivement SV, SV^2, SV^3 et S^2V, S^2V^2, S^2V^3.

En tournant autour de l'axe des x, on obtient U, SU, S^2U, et l'on en déduit, au moyen de rotations autour de l'origine, les symboles restants UV, UV^2, UV^3; SUV, SUV^2, SUV^3; S^2UV, S^2UV^2, S^2UV^3.

75. Pour avoir la représentation plane du groupe icosaédrique, il convient avant tout de déterminer les projections des sommets du polyèdre. Reportons-nous aux figures 6 et 7. Le centre de projection étant 12 se projette au point à l'infini et le sommet 1 à

Fig. 12.



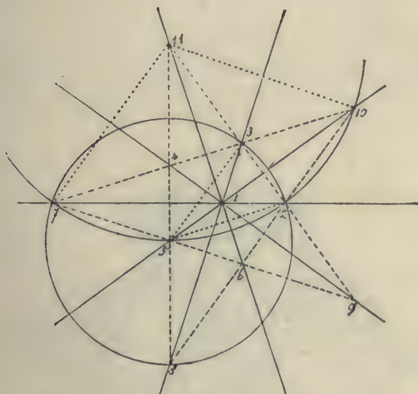
l'origine. La projection du sommet 2 est sur la partie positive de l'axe des x à une distance de l'origine égale au segment O″H″ (*fig.* 7), tandis que la projection du sommet 7 se trouve sur la partie négative de l'axe des x à une distance de l'origine égale à O″K″ [1]. Les projections des autres sommets forment respectivement avec celles des sommets 2 et 7 deux pentagones réguliers ayant l'origine pour centre. Observons que les points 4, 5, 8, 11, situés (n° 65) sur un cercle passant par le centre de projection 12, doivent avoir leurs projections en ligne droite. On peut en dire autant des points 5, 6, 9, 7; 6, 2, 10, 8; 2, 3, 11, 9; 3, 4, 7, 10. Par suite, les points 7, 8, 9, 10, 11 sont les sommets d'un polygone

(1) Si la sphère a pour rayon l'unité, on trouve $OH'' = \frac{r-1}{2}$, $OK'' = \frac{r+1}{2}$.

étoilé, dont les côtés sont les prolongements de ceux du polygone convexe 2, 3, 4, 5, 6.

Cherchons maintenant les projections des cercles de symétrie. Ceux qui passent par les points 1 et 12 se projettent suivant cinq droites issues de l'origine, parmi lesquelles l'axe des x, et faisant

Fig. 13.



entre elles des angles égaux. Considérons, par exemple, le cercle de symétrie contenant les sommets 2, 3, 7, 8. Il se projette, bien entendu, suivant un cercle passant par les projections de ces sommets, et qui, comme nous allons le démontrer, a pour centre le point 5.

Il est évident que

$$5.2 = 5.3 \qquad \text{et} \qquad 5.7 = 5.8;$$

de plus, les angles 5.3.7 et 5.7.3 ont tous deux pour amplitude $\frac{\pi}{5}$ (¹), par suite $5.3 = 5.7$. De même 6, 2, 3, 4 sont les centres des projections des quatre autres cercles de symétrie.

Considérons, au contraire, le cercle de symétrie passant par les

(¹) Il suffit de remarquer que 5.3.7 est l'angle à la base du triangle isoscèle 4.3.5 formé par deux côtés et une diagonale du pentagone régulier convexe 2.3.4.5.6 et que 5.7.3 est un angle du pentagone régulier étoilé 7.8.9.10.11.

sommets 2, 10, 7, 5. Démontrons que le centre de sa projection est le point 11. On voit de suite que

$$11.2 = 11.5 \quad \text{et} \quad 11.7 = 11.10.$$

De plus, comme

$$11.7.10 = 10.7.9 = \frac{\pi}{5},$$

$$11.5.7 = \pi - 4.5.6, \qquad 4.5.6 = \frac{3\pi}{5},$$

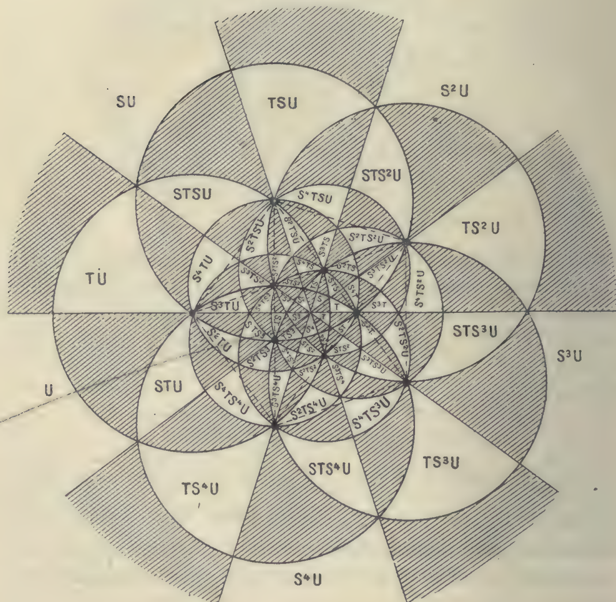
on a

$$11.7.5 = \frac{2\pi}{5} = 11.5.7;$$

d'où

$$11.5 = 11.7.$$

Fig. 14.



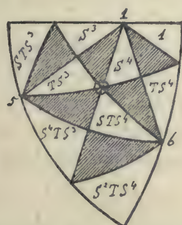
De même 7, 8, 9, 10 sont les centres des projections d'autant de cercles de symétrie.

En résumé, la représentation du groupe icosaédrique comprend cinq droites issues de l'origine et dix cercles égaux cinq à cinq ayant leurs centres aux points 2, 3, ..., 11.

Couvrons de hachures la moitié des triangles curvilignes, et prenons comme triangle initial 1 celui dont un sommet se trouve au point 1 et un côté placé sur la partie positive de l'axe des x. Tournant autour du point 1, nous pourrons marquer les triangles S, S^2, S^3, S^4.

En tournant autour du milieu de l'arête 1.2, nous aurons T, et nous obtiendrons, en tournant autour du point 2 et en vertu d'une remarque déjà faite (n° 66), les triangles ST, S^2T, S^3T, S^4T.

Fig. 15.



Tournons au contraire autour de 1, nous déduirons de T les triangles TS, TS^2, TS^3.

Et pareillement de $S^hT(h = 1, 2, 3, 4)$ les triangles S^hTS, S^hTS^2, S^hTS^3, S^hTS^4.

Enfin, appliquant aux 30 triangles déjà marqués une rotation π autour de l'axe des y, nous obtiendrons finalement les triangles ayant pour symboles S^hU et $S^hTS^kU(h, k = 0, 1, 2, 3, 4)$.

Nous avons déjà eu l'occasion de considérer les cinq systèmes de trois médianes orthogonales de l'icosaèdre (n° 67). Les extrémités de chaque système sont les sommets d'un octaèdre régulier, et les centres sphériques des faces des cinq octaèdres sont des points appartenant à l'ensemble des centres sphériques des faces de l'icosaèdre, comme cela résulte, en toute évidence, de la figure 15 où est reproduite et agrandie la partie de la figure 14 formée

d'une face de l'octaèdre h_1 correspondant au système k_1 (¹).

Puisqu'il y a en tout 40 faces pour des octaèdres et 20 faces pour l'icosaèdre, le centre sphérique de chaque face de l'icosaèdre est centre sphérique de deux des faces des octaèdres.

Considérations générales sur les réseaux de triangles.

76. Chacun des réseaux de triangles qu'on vient de construire possède les propriétés suivantes (²) :

1° Il peut être engendré par symétrie en partant d'un quelconque des triangles qui le constituent;

2° Tous les triangles ont les mêmes angles qui sont égaux à des sous-multiples de π;

3° Le réseau recouvre le plan une seule fois, c'est-à-dire que deux figures du réseau n'empiètent jamais l'une sur l'autre;

4° Il recouvre le plan tout entier;

5° Il se compose d'un nombre fini de triangles;

6° Tous les angles groupés autour d'un sommet commun sont égaux.

Nous rencontrerons dans la suite des réseaux ne possédant que quelques-unes des propriétés précédentes. Aussi appellerons-nous réseaux *réguliers* ceux qui possèdent la propriété 6° et réseaux *finis* ceux qui possèdent la propriété 5°.

Pour l'instant étudions la nature d'un réseau répondant aux conditions 1° et 3°. Considérons un des sommets du triangle générateur; il appartiendra à d'autres triangles alternativement égaux et symétriques. Or, le réseau ne doit pas se recouvrir lui-même; donc, après avoir rencontré un nombre pair de triangles, y compris le triangle primitif, on devra retomber sur ce dernier triangle.

(¹) Cette figure montre en effet que les quinze triangles composant la face de l'octaèdre sont disposés de la même façon autour du centre sphérique de la face 1.5.6 de l'icosaèdre, centre qu'on a mis en évidence sur la figure en l'entourant d'un petit cercle.

(²) Il m'a paru utile de faire remarquer que ces propriétés ne sont pas toutes indépendantes.

On voit que, autour du sommet considéré, tous les angles seront égaux à un même sous-multiple de π. Donc :

Un réseau, ne se recouvrant jamais lui-même et formé de triangles qui se déduisent de l'un d'eux par symétrie, est un réseau régulier; et les triangles de ce réseau ont pour angles des sous-multiples de π.

Il peut arriver qu'un tel réseau ne possède pas les propriétés 4° et 5°.

Considérons un des réseaux finis déjà étudiés. Nous savons que, s'il comprend $2n$ triangles dont les angles sont $\frac{\pi}{\nu_1}, \frac{\pi}{\nu_2}, \frac{\pi}{\nu_3}$, on a

$$\frac{\pi}{\nu_1}+\frac{\pi}{\nu_2}+\frac{\pi}{\nu_3}=\pi+\frac{2\pi}{n};$$

d'où

$$\frac{\pi}{\nu_1}+\frac{\pi}{\nu_2}+\frac{\pi}{\nu_3}>\pi \quad [1],$$

ou bien

$$(a) \qquad \frac{1}{\nu_1}+\frac{1}{\nu_2}+\frac{1}{\nu_3}>1.$$

Supposons maintenant que l'on se donne un triangle dont les angles $\frac{\pi}{\nu_1}, \frac{\pi}{\nu_2}, \frac{\pi}{\nu_3}$ ne satisfassent pas à la condition (a).

Deux cas pourront se présenter :

$$(b) \qquad \frac{1}{\nu_1}+\frac{1}{\nu_2}+\frac{1}{\nu_3}=1,$$

$$(c) \qquad \frac{1}{\nu_1}+\frac{1}{\nu_2}+\frac{1}{\nu_3}<1.$$

Pour distinguer facilement ces trois cas, procédons ainsi. Soient a, b, c les trois côtés du triangle; α, β, γ les sommets qui leur sont respectivement opposés. Si le triangle a deux côtés non rectilignes, b et c par exemple, soit α_1 le second point d'intersection des cercles auxquels ils appartiennent. Faisons une inversion (n° 19) de pôle α_1. Les cercles dont font partie b et c

---

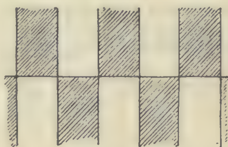
[1] Cette relation est immédiate si l'on remarque que la somme des angles d'un triangle sphérique est supérieure à deux droits et que chacun des triangles considérés, étant la projection stéréographique d'un triangle sphérique, a les mêmes angles que ce triangle sphérique.

se transforment en droites, et nous obtenons un nouveau triangle dont deux côtés au moins sont rectilignes et dont les angles sont égaux à ceux du premier. Ce triangle a son troisième côté rectiligne dans le cas (b), curviligne et tournant sa concavité vers le côté opposé dans le cas (a), sa convexité dans le cas (c).

77. Le cas (a) a déjà été examiné complètement.

Passons au cas (b); si l'on suppose $\nu_1 \leqq \nu_2 \leqq \nu_3$, il est clair qu'on doit avoir $\nu_1 \leqq 3$.

Fig. 16.



Si $\nu_1 = 2$, on a

$$\frac{1}{\nu_2} + \frac{1}{\nu_3} = \frac{1}{2},$$

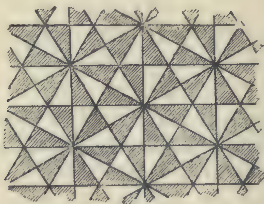
d'où

$$2 \leqq \nu_2 \leqq 4,$$

et, par suite, les trois solutions

$$\nu_2 = 2, \quad \nu_3 = \infty; \quad \nu_2 = 3, \quad \nu_3 = 6 \quad \nu_2 = \nu_3 = 4.$$

Fig. 17.



Si $\nu_1 = 3$, on a

$$\frac{1}{\nu_2} + \frac{1}{\nu_3} = \frac{2}{3},$$

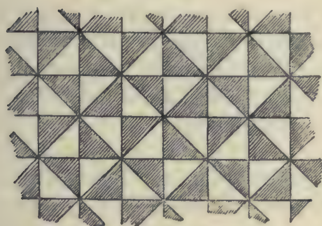
et, comme on a nécessairement $\nu_2 \leqq 3$, on obtient la seule solution

$$\nu_2 = \nu_3 = 3.$$

En résumé, le cas (b) donne lieu aux 4 types

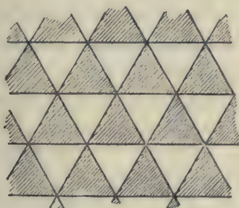
$$\nu_1 = 2, \quad \nu_2 = 2, \quad \nu_3 = \infty,$$
$$\nu_1 = 2, \quad \nu_2 = 3, \quad \nu_3 = 6,$$
$$\nu_1 = 2, \quad \nu_2 = 4, \quad \nu_3 = 4,$$
$$\nu_1 = 3, \quad \nu_2 = 3, \quad \nu_3 = 3.$$

Fig. 18.



Nous avons figuré les quatre réseaux correspondants; ils possèdent toutes les propriétés énoncées au n° 76, sauf la cinquième; ce sont des réseaux infinis.

Fig. 19.

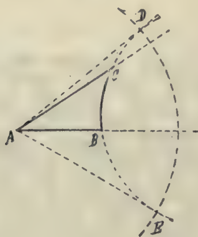


Si l'on passe maintenant au cas plus général d'un triangle fondamental quelconque n'ayant plus deux côtés rectilignes, on aura, au lieu de droites, c'est-à-dire de cercles passant par le point à l'infini, une infinité de cercles passant tous par le même point. On peut donc dire que le cas (b) donne lieu à des réseaux infinis recouvrant tout le plan et formés de cercles passant tous par un même point.

78. Le cas (c) donne lieu évidemment à un nombre infini de types.

Soit ABC le triangle donné, où l'on suppose AB et AC rectilignes, BC circulaire et tournant sa convexité vers A. De A nous pourrons mener deux tangentes au cercle contenant BC, et

Fig. 20.



l'angle BAC sera intérieur à l'angle DAE ou pourra tout au plus coïncider avec lui (si les angles B et C sont nuls). Le cercle de centre A, passant par D et E, coupera donc orthogonalement les prolongements des trois côtés du triangle donné.

Construisons le triangle symétrique de ABC par rapport à l'un de ses côtés. Le cercle DE étant orthogonal aux trois côtés est son propre symétrique par rapport à l'un quelconque d'entre eux, et, puisque la symétrie conserve les angles, il coupe encore orthogonalement le prolongement des trois côtés du nouveau triangle. On en conclut que :

Dans un réseau du type (*c*), *tous les côtés sont orthogonaux à un même cercle et sont situés d'un même côté de ce cercle ; s'il y a des angles nuls, les sommets correspondants, et ceux-là seulement, sont situés sur le cercle.*

On voit, d'après cela, que ces derniers réseaux ont la propriété 4° du n° 76 ; ils recouvrent en effet seulement l'une des deux régions en lesquelles le plan est partagé par un certain cercle.

Un réseau spécial du type (*c*) nous occupera d'ici peu ; c'est le réseau représentatif du *groupe modulaire*.

79. *Un réseau de triangles est l'image d'un groupe de substitutions linéaires et de son groupe amplifié.*

Soient a un triangle du réseau, b un autre triangle blanc du réseau se déduisant de a par symétrie. On passe de a à b par un nombre pair de transformations par symétrie; mais chacune d'elles est (nº 41) l'image d'une pseudosubstitution, et, comme le produit d'un nombre pair de pseudosubstitutions est une substitution, on voit qu'on passe de a à b au moyen d'une substitution linéaire. Donc, si l'on se donne un réseau, on peut lui faire correspondre un ensemble de substitutions linéaires : ce sont les substitutions qui changent le réseau en lui-même. Si l'on regarde un des triangles blancs comme triangle primitif, il existe une correspondance biunivoque entre les substitutions de l'ensemble et les triangles blancs du réseau.

Il est clair que l'ensemble des substitutions ainsi formées est indépendant du triangle du réseau choisi pour triangle primitif.

Appelons S la substitution qui transforme a et b, et soit c un troisième triangle blanc. Puisque b peut être aussi considéré comme triangle fondamental, il existera une substitution S′ de l'ensemble changeant b en c. Le produit SS′ sera une substitution changeant a en c, et, comme dans l'ensemble considéré il existe une substitution et une seule S″ ayant cette propriété, on aura

$$S'' = SS'.$$

Les substitutions trouvées forment donc un groupe G. Ce groupe contient évidemment l'identité; de plus, il renferme l'inverse de chacune de ses substitutions.

En effet, en considérant a comme triangle fondamental, S est la substitution changeant a en b; inversement, si l'on prend b comme triangle fondamental, S^{-1} sera la substitution changeant b en a.

Il est évident ensuite que l'ensemble des opérations transformant un triangle blanc déterminé du réseau en tous les autres triangles tant blancs qu'ombrés n'est autre que le groupe amplifié $\overline{G}$.

Appelons *bitriangle* la figure formée par deux triangles adjacents et supposons que nos bitriangles aient eux-mêmes la forme triangulaire [1]; soient a le triangle générateur, a_1, a_2, a_3 les

[1] Cela a toujours lieu quand les triangles ont un angle droit, et dans ce cas seulement.

bitriangles qui lui sont adjacents; S_1, S_2, S_3 les substitutions changeant a respectivement en a_1, a_2, a_3. Les produits composés avec les substitutions précédentes changeront a_1, a_2, a_3 en des triangles respectivement adjacents, et ainsi de suite. Comme le réseau constitue un champ connexe, la substitution changeant a en un bitriangle quelconque b du réseau pourra s'exprimer à l'aide d'un produit renfermant les seules substitutions S_1, S_2, S_3. Ces dernières substitutions sont dites les *substitutions génératrices* du groupe ([1]).

80. Nous dirons que deux points du plan sont *homologues* dans un groupe d'opérations, s'il existe une opération du groupe transformant l'un d'eux dans l'autre. Deux champs formés de points respectivement homologues sont dits *homologues*.

L'homologie jouit des trois propriétés fondamentales de l'égalité, pourvu que le groupe renferme l'opération identique et l'inverse de chacune de ses opérations. En effet :

a. Tout point est son propre homologue, puisque le groupe contient l'opération identique permettant de passer d'un point quelconque au même point;

b. Si A *est homologue de* B, B *est homologue de* A, car, si l'opération P du groupe change A en B, l'opération P^{-1} appartient au même groupe et change B en A;

c. Si A *est homologue de* B *et si* B *est homologue de* C, A *est homologue de* C, car, si P change A en B et si Q change B en C, PQ appartient encore au groupe et change A en C.

Relativement à un groupe de substitutions d'ordre fini n, les points d'un plan se partagent en système des n points homologues. Il y a exception pour les nœuds du réseau, ceux-ci formant respectivement des systèmes de $\frac{n}{\nu_1}$, $\frac{n}{\nu_2}$, $\frac{n}{\nu_3}$ points homologues.

Donc, en considérant les nœuds comme des points multiples d'ordre ν_i, on peut dire que, *par rapport à un groupe de substi-*

([1]) Il n'est pas inutile de remarquer que S_1, S_2, S_3 ne sont pas nécessairement indépendantes entre elles. Si les bitriangles n'avaient pas la forme triangulaire, le nombre des substitutions génératrices serait supérieur à 3.

tutions d'ordre n, un point quelconque du plan appartient à un système de n points homologues.

81. Soient un réseau de triangles et *a* un quelconque de ses bitriangles; *un point intérieur à a n'a pas d'autre homologue dans a que lui-même, mais il a un homologue dans chacun des autres bitriangles.*

Au contraire, un point situé sur l'un des côtés du bitriangle *a*, pouvant être considéré comme appartenant aussi au bitriangle adjacent, aura son homologue sur le contour de *a*. Donc, *chaque point du contour de a, et qui n'est pas un sommet, a un homologue et un seul sur ce même contour* (cet homologue, dans certains cas, pouvant coïncider avec le point donné).

Enfin, un sommet de a a pour homologues autant de sommets de a (non nécessairement distincts) *qu'il y a de bitriangles se croisant en ce point.*

Soit donc un bitriangle quelconque; ne conservons de son contour qu'une portion convenablement choisie. Nous obtenons un champ connexe possédant la propriété de ne renfermer aucun couple de points homologues et de contenir un point homologue de chaque point du réseau.

Un tel champ est dit *champ fondamental.*

Pour un réseau donné, le champ fondamental peut être choisi de bien des façons. En effet, soient l, l' deux parties homologues du contour n'ayant aucun point commun; on peut retrancher du bitriangle une région attenant à l, et la remplacer par la partie homologue du réseau s'appuyant sur l'. La figure ainsi obtenue, moyennant les conventions relatives au contour, est encore un champ fondamental. Des modifications de ce genre, permettant de passer d'un champ fondamental à un autre, sont dites *modifications permises.*

82. Soient un réseau, G le groupe de substitutions linéaires qui lui correspond, H un sous-groupe de G d'indice fini *s*. Reprenons les notations du n° 9. Soient

$$P_0 = 1, \ P_1, \ P_2, \ \ldots$$

les substitutions de H. Celles de G pourront être rangées dans un

Tableau de la forme suivante :

$$(1)\quad \left\{\begin{array}{lllll} & P_0 = 1, & P_1, & P_2, & \ldots, \\ Q_1 & P_0 = Q_1, & Q_1 P_1, & Q_1 P_2, & \ldots, \\ Q_2 & P_0 = Q_2, & Q_2 P_1, & Q_2 P_2, & \ldots, \\ \ldots & \ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, \\ Q_{s-1} & P_0 = Q_{s-1}, & Q_{s-1} P_1, & Q_{s-1} P_2, & \ldots \end{array}\right.$$

Représentons par 1 le bitriangle générateur du réseau, que nous supposerons de forme triangulaire. Soient S_1, S_2, S_3 les symboles des bitriangles adjacents à (1) et qu'on déduit de 1 en lui appliquant les substitutions S_1, S_2, S_3 génératrices du groupe G. Relativement à H, ces triangles ne peuvent être tous les trois homologues du bitriangle 1; sinon H contiendrait les substitutions S_1, S_2, S_3, par suite toutes les substitutions de G, et se confondrait alors avec G.

Supposons, par exemple, que 1 soit homologue de S_2, S_3 et non de S_1; et soient S_{12}, S_{13} les bitriangles autres que 1, adjacents à S_1. Si S_{12} et S_{13} sont homologues de 1 ou de S_1, nous limiterons nos considérations au champ formé par les bitriangles 1, S_1. Si, au contraire, S_{12}, par exemple, n'est homologue ni de 1, ni de S_1, nous considérerons le champ formé par les bitriangles 1, S_1, S_{12}. Et nous continuerons toujours de la même façon. Je dis que l'application de ce procédé donnera lieu à un nombre fini d'opérations. En effet, les bitriangles correspondant aux substitutions d'une même ligne du Tableau (1) étant homologues dans H, après avoir rencontré au plus s bitriangles non homologues, on retombera nécessairement sur des bitriangles homologues de certains des précédents. Nous sommes donc conduits à former un champ connexe C, composé de bitriangles, dont s au plus non homologues entre eux. Si nous démontrons que chaque point du réseau a un homologue dans C, il en résultera que C est composé précisément de s bitriangles; car, si le nombre de bitriangles était inférieur à s, il existerait une ligne du Tableau (1) pour laquelle aucun des bitriangles correspondants n'appartiendrait à C et alors certains points du réseau n'auraient pas d'homologue dans C.

Pour établir notre assertion, faisons une remarque préliminaire. Soient a un bitriangle extérieur, mais attenant au champ C; b le triangle intérieur à C et attenant à a. Du moment que a est

extérieur à C, c'est qu'il existe dans C un bitriangle a' homologue de a. Parmi les bitriangles contigus à a', il doit y en avoir un, soit b', homologue de b; mais il est nécessairement extérieur à C, puisque b est intérieur; par suite b' s'appuie sur le contour de C. Nous avons donc sur le contour de C deux arcs homologues, séparant respectivement a de b et a' de b'.

Le raisonnement précédent montre que les points du contour de C sont deux à deux homologues dans le groupe H.

Cela posé, soit z un point quelconque de la région du plan recouverte par le réseau. Prenons un point quelconque z_0 intérieur à C, et joignons z_0 à z par une ligne l qui ne sorte pas du champ occupé par le réseau et qui rencontre un nombre fini de triangles. Soient z_1 le point où l rencontre pour la première fois le contour de C; a_1, a_2, ... les bitriangles extérieurs à C qu'elle traverse successivement; l_1, l_2, ... les portions de cette ligne comprises respectivement dans ces bitriangles; m la portion aboutissant à z.

D'après ce qui précède, il existera sur le contour de C un point z'_1 homologue de z_1, et l'on pourra tracer à l'intérieur de C et à partir de z'_1 une ligne l'_1 homologue de l_1, puis une ligne l'_2 homologue de l_2 et ainsi de suite. Le tracé sera achevé après un nombre fini d'opérations, et l'extrémité de la portion m' homologue de m sera le point homologue de z dans le champ C.

Donc, tout point du réseau a un homologue dans C. En définitive : *Si* H *est un sous-groupe de* G *d'indice fini s, on peut, à l'aide de s bitriangles du réseau représentatif de* G, *constituer pour* H *un champ fondamental* C.

Le réseau entier correspondant à G pourra être décomposé en champs homologues de C relativement à H; ces champs formeront le réseau (polygonal) relatif au groupe H et l'on pourra dire que ce réseau est *contenu* dans celui de G, en ce sens que les côtés et les nœuds de H seront aussi des côtés et des nœuds de G, sans que l'inverse ait lieu. On peut en conclure que : *Étant donnés un groupe et un de ses sous-groupes, le réseau du second est contenu dans celui du premier.*

83. Soit H' un sous-groupe de G équivalent à H, par exemple

$$H' = S^{-1} H S.$$

Soient z, z' deux points homologues dans H; Sz, Sz' sont alors homologues dans H' (n° 2). Si donc on applique au champ la substitution S, le champ $C' = SC$ ainsi obtenu est un champ fondamental pour le sous-groupe H'. Plus simplement, si l'on désigne maintenant par le symbole S le triangle qu'on avait désigné primitivement par le symbole 1, C devient un champ fondamental de H'. Et comme dans ces conditions le symbole 1 s'applique alors au triangle désigné primitivement par S^{-1} ou à son homologue dans C, on en conclut que : *Le champ* C *peut être considéré comme le champ fondamental de divers sous-groupes équivalents en assignant le symbole* 1 *successivement à chacun de ses bitriangles.*

On déduit de là la conséquence importante suivante : *Soient* H *un sous-groupe invariant de* G, S *une substitution quelconque de* G *et* C *un champ fondamental de* H; SC *est encore un champ fondamental de* H; *en d'autres termes* S *transforme* C *en lui-même, aux modifications permises près* ([1]).

Un artifice géométrique permet de présenter ces résultats sous une forme plus simple.

On a vu que le contour de C se compose de portions deux à deux homologues.

Transformons C par une déformation continue en une surface fermée, en amenant en coïncidence puis soudant ensemble les parties homologues de son contour. Il est clair que si, au lieu de partir de C, nous partions d'une figure déduite de C par des modifications permises, nous obtiendrons encore la même surface fermée. Ainsi, tandis que la disposition des triangles dans le champ fondamental comporte beaucoup d'arbitraire, cet arbitraire disparaît quand on passe à la surface fermée; en sorte que relativement à cette surface il n'y a pas lieu de parler de modifications permises. On peut donc dire que :

Si H *est un sous-groupe invariant d'un groupe* G, *la sur-*

([1]) Ces considérations s'appliquent à H, si on le considère comme sous-groupe du groupe amplifié $\overline{G}$. Ainsi : *Soient* H *un sous-groupe invariant de* G *et* $\overline{G}$, *et* R *la réflexion utilisée pour l'amplification;* C *est symétrique par rapport au cercle de symétrie de* R, *aux modifications permises près.*

Il est clair que réciproquement, *si* H *est un sous-groupe invariant de* G *et que* C *soit ou puisse être rendu, par des modifications permises, symétrique par rapport au cercle de symétrie de* R, H *est un sous-groupe invariant de* $\overline{G}$.

face fermée déduite du champ fondamental de H *est transformée en elle-même par toute substitution de* G.

Le nombre des différentes transformations de la surface en elle-même est évidemment égal au nombre s des bitriangles qu'elle renferme ou encore à l'indice du sous-groupe, car on peut transformer le bitriangle 1 en chacun des s bitriangles y compris le bitriangle 1 lui-même, et, d'autre part, une fois fixé le bitriangle transformé de 1, la transformation est définie sans ambiguïté.

Appelons *nœuds de première, deuxième et troisième espèce* les nœuds correspondant respectivement aux sommets des angles d'amplitude $\frac{\pi}{\nu_1}, \frac{\pi}{\nu_2}, \frac{\pi}{\nu_3}$. Puisque les transformations de la surface en elle-même échangent entre eux les nœuds de même espèce, on peut dire que :

Étant donné un sous-groupe invariant, la surface correspondante est telle que, autour de chacun des nœuds, se croisent des triangles dont le nombre ne varie pas pour des nœuds de même espèce.

On exprime ce fait en disant que la surface est *régulière*.

84. Revenons au Tableau du n° 82 et rappelons que les s bitriangles du champ C ont pour symboles s substitutions appartenant respectivement aux s lignes du Tableau.

Nous pouvons alors attribuer aux s bitriangles les symboles respectifs

$$(2) \qquad 1, \; Q_1, \; Q_2, \; \ldots, \; Q_{s-1},$$

aux substitutions près de H, en entendant par là que le véritable symbole du triangle désigné par Q_i n'est pas nécessairement Q_i, mais peut être le produit de Q_i par une substitution de H. Si nous transformons ensuite le champ en une surface fermée et que nous superposions tous les champs homologues de C, qui composent le réseau et cela en faisant coïncider les bitriangles homologues [1], le bitriangle Q_i représentera, à lui seul, tous les

[1] N'oublions pas que nous admettons qu'on peut déformer nos figures d'une façon quelconque, pourvu que la continuité soit respectée.

triangles dont les symboles figurent dans la ligne de rang $i+1$ du Tableau (1). D'après cela, les symboles (2) peuvent représenter s transformations de la surface en elle-même, Q_i étant le symbole de la transformation produite par une quelconque des substitutions $Q_i P_h (h = 0, 1, 2, \ldots)$, transformation qui est indépendante de l'indice h.

Ces s transformations forment un groupe quand H *est un sous-groupe invariant.*

En effet, puisque, dans ce cas, quels que soient les indices α, β, il existe toujours un troisième indice β' tel que

$$Q_\alpha^{-1} P Q_\alpha = P_{\beta'}$$

ou

$$P_\beta Q_\alpha = Q_\alpha P_{\beta'},$$

on peut écrire

$$Q_i P_h Q_j P_k = Q_i Q_j P_{h'} P_k;$$

mais $Q_i Q_j$ est une certaine substitution de G, figurant par conséquent dans le Tableau (1) (n° 82); elle est par suite de la forme $Q_l P_m$, donc

$$Q_i P_h Q_j P_k = Q_l P_m P_{h'} P_k.$$

Et comme $P_m P_{h'} P_k$ est une certaine substitution P_r du sous-groupe H

$$Q_i P_h Q_j P_k = Q_l P_r,$$

où l dépend seulement de i et de j, nous écrirons ce résultat sous la forme symbolique suivante

$$Q_i Q_j = Q_l,$$

dont la signification apparaît immédiatement, si par Q_i on entend, non pas la substitution qu'elle représente, mais la transformation correspondante de la surface fermée en elle-même.

Le groupe G′ des transformations de la surface en elle-même est mériédriquement isomorphe au groupe G et le degré de mériédrie est égal à l'ordre du sous-groupe H, quand celui-ci est fini. A la substitution identique de G′ correspond dans G le sous-groupe H; à un sous-groupe G′ correspond un sous-groupe de G renfermant H. Et comme l'étude de G′ est toujours plus facile que celle de G, on voit qu'il y a un réel avantage à ramener la recherche des sous-groupes de G à celle des sous-groupes de G′.

85. Pour bien faire comprendre les développements précédents, donnons un exemple que nous utiliserons plus tard.

On a vu (n° 54) que le groupe trirectangle est un sous-groupe invariant du groupe octaédrique. Désignons ces deux groupes respectivement par H et G. Les substitutions du groupe H sont

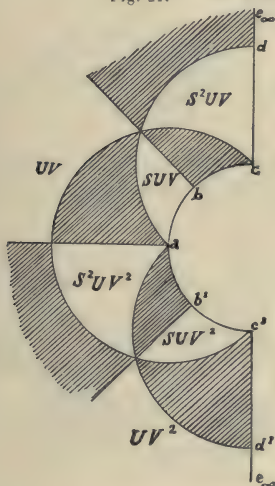
$$1, \quad V^2, \quad U, \quad UV^2.$$

Partons d'un quelconque des bitriangles du réseau octaédrique, par exemple de UV. Ceux qui lui sont adjacents sont U, UV^2, S^2UV^2; les deux premiers sont homologues dans H, donc il suffit de retenir UV^2 et S^2UV^2. Les bitriangles qui leur sont contigus et qui sont en même temps distincts de UV sont

$$UV^3, \quad S^2UV^3, \quad SUV, \quad SUV^2;$$

UV^3 est homologue de UV, donc nous retenons les trois autres.

Fig. 21.

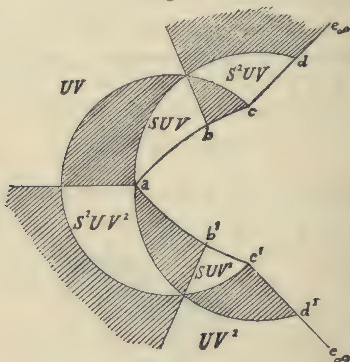


Nous obtenons ainsi un champ fondamental de H composé des six bitriangles suivants :

(1) $UV, \quad UV^2, \quad S^2UV^2, \quad S^2UV^3, \quad SUV, \quad SUV^2.$

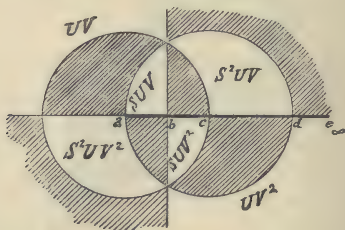
Si à la moitié ombrée de UV^2 et à la moitié blanche de S^2UV^3 nous substituons la moitié ombrée de U et la moitié blanche de S^2UV qui leur sont respectivement homologues dans H, nous obtenons le champ fondamental représenté par la figure 21. Les portions homologues sur le contour sont deux à deux : ab, $a'b'$, bc, $b'c'$, cd, $c'd'$, de, $d'e'$.

Fig. 22.



Déformons le réseau comme cela est indiqué sur la figure 22, de façon à amener la coïncidence des côtés homologues.

Fig. 23.



Il peut se ramener à la forme de la figure 23, qui représente, comme il est facile de le voir, un réseau diédrique de douze triangles ($m = 3$) projeté stéréographiquement en prenant comme point de vue l'un des nœuds placé sur l'équateur.

Il résulte de là que, si l'on forme le Tableau (1) du n° 82, et si l'on choisit un élément dans chacune des lignes, les six éléments ainsi obtenus doivent former un groupe diédrique aux substitutions de H près.

En tenant compte des relations établies dans la note (p. 80), le Tableau s'écrit

$$(2)\quad \left\{\begin{array}{llll} 1, & V^2, & U, & UV^2, \\ V, & V^3, & UV^3, & UV, \\ S, & SV^2, & SU, & SUV^2, \\ SV, & SV^3, & SUV^3, & SUV, \\ S^2, & S^2V^2, & S^2U, & S^2UV^2, \\ S^2V, & S^2V^3, & S^2UV^3, & S^2UV. \end{array}\right.$$

On peut observer que les six substitutions (1) appartiennent à six lignes diverses du Tableau. Et comme V^2 est homologue de 1 dans H, on voit immédiatement que les six substitutions

$$1,\quad S,\quad S^2,\quad V,\quad SV,\quad S^2V$$

forment un groupe diédrique, aux substitutions de H près.

On peut encore suivre une marche inverse. Puisque les six substitutions 1, S, S^2, V, SV, S^2V forment, aux substitutions de H près, un groupe diédrique, on peut partir du réseau représentatif de ce groupe (*fig.* 23), fendre suivant la ligne *abcde* la surface sur laquelle est tracé ce réseau; on déforme ensuite la surface, comme cela est indiqué sur la figure 22, et on lui donne enfin la forme indiquée par la figure 21, les parties homologues du contour étant les deux bords de la coupure pratiquée dans la surface fermée.

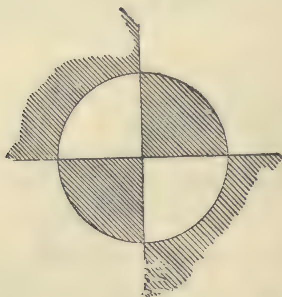
On voit sans difficulté que le réseau octaédrique se divise en quatre parties homologues relativement à H : celle qui est tracée dans la figure 21, sa symétrique par rapport à l'axe imaginaire et les deux demi-cercles en lesquels le cercle de rayon 1 est partagé par cet axe. Ces quatre parties, considérées comme bitriangles et partagées en triangles par l'axe réel, nous donnent le réseau du groupe trirectangle.

86. Déterminons maintenant le genre p de la surface fermée correspondant à un sous-groupe d'indice s.

Le théorème d'Euler (n° 52) généralisé [1] donne, ou une surface fermée de genre p,

$$F + S = A + 2 - 2p.$$

Fig 24.



Appelons $2m_1, 2m_2, \ldots, 2m_S$ le nombre des arêtes aboutissant à chacun des sommets ; on aura

$$A = \sum_{i=1}^{S} m_i.$$

---

[1] Voici comment on peut démontrer cette formule :

Soit $e_h (h \geqq 3)$ le nombre des nœuds où aboutissent h arêtes ; on a

$$S = \sum_h e_h ;$$

de plus, comme chaque arête a deux extrémités, on aura

$$A = \frac{1}{2} \sum_h h e_h.$$

Un point où se croisent h arêtes peut être considéré comme provenant de la coïncidence de $h - 2$ points de concours des arêtes deux à deux. Ainsi, dans la figure 25, p provient de la coïncidence des trois points p_1, p_2, p_3. Coupons, par exemple, l'arête ap en un point o ; les deux portions de cette arête et toutes les autres arêtes pourront être considérées comme autant de coupures de première espèce. Considérons les extrémités de ces coupures ; deux tombent en o et $h - 2$ en p, de sorte que le nombre total des extrémités est

$$2 + \sum (h - 2) e_h$$

En outre, les faces sont ici en nombre $2s$; par suite

$$2s + S = \sum_{i=1}^{S} m_i + 2 - 2p,$$

d'où

$$p = 1 - s + \frac{1}{2}\sum_{i=1}^{S}(m_i - 1).$$

Si le sous-groupe est invariant, la surface est régulière et m_i a la même valeur pour tous les sous-groupes de même espèce.

Appelons n_1, n_2, n_3 les valeurs de m_i pour les nœuds de première, deuxième et troisième espèces.

Comme un nœud de $i^{\text{ième}}$ espèce, où concourent $2n_i$ arêtes, appartient à n_i triangles blancs, on voit que le nombre des nœuds de cette espèce situés sur la surface fermée est $\frac{s}{n_i}$ [1] et la formule précédente devient alors

$$(1) \qquad p = 1 - s + \sum_{i=1}^{3} \frac{s}{n_i}\,\frac{n_i - 1}{2}.$$

---

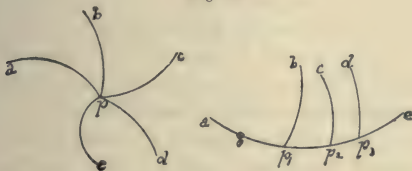
et celui des coupures

$$1 + \frac{1}{2}\sum (h-2)e_h$$

ou bien

$$A - S + 1.$$

Fig. 25.



Ces coupures décomposent la surface en F parties, d'où, d'après un théorème connu,

$$F = (A - S + 1) - 2p + 1$$

ou bien

$$F + S = A + 2 - 2p.$$

(1) En effet, comme un point de la surface admet en général s points homologues, y compris le point lui-même, un nœud de $i^{\text{ème}}$ espèce, appartenant à n triangles blancs, n'admet que $\frac{s}{n_i}$ points homologues.

Ajoutons que n_1, n_2, n_3 sont nécessairement des sous-multiples de s, et qu'ils sont aussi des sous-multiples respectivement de ν_1, ν_2, ν_3.

Le groupe modulaire et les sous-groupes correspondants.

87. Le groupe modulaire admet une définition arithmétique très simple. Cependant il est plus conforme au point de vue actuel de se donner le champ fondamental et d'en déduire les propriétés arithmétiques du groupe.

Considérons dans le demi-plan supérieur le triangle formé par l'axe des quantités imaginaires, la parallèle à cet axe d'abscisse $-\frac{1}{2}$ et le cercle de rayon *un* ayant pour centre l'origine. Ce triangle a pour sommets les points

$$i, \qquad \rho = \frac{-1 + i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$$

et le point à l'infini; ses angles sont $\frac{\pi}{2}$, $\frac{\pi}{3}$ et o; par suite

$$\nu_1 = 2, \qquad \nu_2 = 3, \qquad \nu_3 = \infty.$$

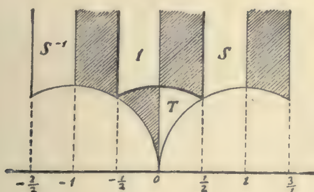
Le réseau formé par ce triangle et ceux qui s'en déduisent par symétrie appartient donc au type (c) du n° 76. Cherchons son cercle de symétrie. Les seuls cercles orthogonaux aux deux côtés parallèles du triangle sont les droites parallèles à l'axe des quantités réelles; et parmi elles la seule qui soit orthogonale au côté curviligne du triangle passe par le centre du cercle auquel appartient ce côté et se confond par conséquent avec l'axe réel. Donc, le cercle de symétrie cherché est l'axe réel et par suite le réseau est situé tout entier dans le demi-plan supérieur. Les sommets des angles nuls, c'est-à-dire les homologues du point à l'infini, sont tous sur l'axe réel.

Nous prendrons pour champ fondamental de notre groupe le bitriangle formé du triangle construit précédemment et de son symétrique par rapport à l'axe imaginaire.

Les parties du contour que nous considérerons comme appartenant au bitriangle sont le côté rectiligne de gauche et la moitié, à droite, du côté circulaire.

Considérons les trois bitriangles contigus; on les obtient respectivement par deux translations de grandeurs $+1$ et -1 et une

Fig. 26.



inversion par rapport au cercle de rayon *un* ayant pour centre l'origine. Les substitutions correspondantes ont pour expression analytique

$$(1)\qquad S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Ces substitutions étant *unitaires* et à *coefficients entiers*, il en sera de même de toutes les substitutions du groupe qu'elles déterminent.

Réciproquement toute substitution unitaire et à coefficients entiers peut être mise sous la forme d'un produit de puissances des substitutions (1).

En effet, soit

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

une substitution dont les éléments α, β, γ, δ sont des entiers liés par la relation

$$(2)\qquad \alpha\delta - \beta\gamma = 1.$$

Comme γ et δ ne peuvent être nuls en même temps, trois cas sont possibles :

$$\gamma \neq 0, \quad \delta = 0; \qquad \gamma = 0, \quad \delta \neq 0; \qquad \gamma \neq 0, \quad \delta \neq 0.$$

Soit d'abord $\gamma \neq 0$, $\delta = 0$. Alors, d'après (2),

$$\beta\gamma = -1,$$

et par suite, en désignant par ε la quantité ± 1,

$$\beta = \varepsilon, \qquad \gamma = -\varepsilon,$$

en sorte que

$$P = \begin{pmatrix} \alpha & \varepsilon \\ -\varepsilon & 0 \end{pmatrix},$$

c'est-à-dire

$$z' = -\varepsilon\alpha - \frac{1}{z}.$$

Posons maintenant

$$-\frac{1}{z} = z_1;$$

on a

$$z' = z_1 - \varepsilon\alpha,$$

c'est à-dire

$$P = TS^{-\varepsilon\alpha}.$$

Soit en second lieu $\gamma = 0$, $\delta \neq 0$. Alors

$$\alpha\delta = 1, \qquad \alpha = \delta = \varepsilon,$$

$$P = \begin{pmatrix} \varepsilon & \beta \\ 0 & \varepsilon \end{pmatrix},$$

c'est-à-dire

$$z' = z + \varepsilon\beta,$$

d'où

$$P = S^{\varepsilon\beta}.$$

Soit enfin $\gamma \neq 0$, $\delta \neq 0$. La relation (2) montre que γ et δ sont premiers entre eux. Développons en fraction continue la fraction irréductible $\frac{\gamma}{\delta}$:

$$\frac{\gamma}{\delta} = k_1 + \cfrac{1}{k_2 + \ddots + \cfrac{1}{k_n}}.$$

Désignons les réduites par la notation

$$\frac{M_i}{N_i} \qquad (i = 0, 1, 2, \ldots, n);$$

les quotients complets sont

$$\frac{M_0}{N_0} = 1, \qquad \frac{M_1}{N_1} = \frac{k_1}{1}, \qquad \frac{M_2}{N_2} = \frac{k_1 k_2 + 1}{k_2}, \qquad \ldots, \qquad \frac{M_n}{N_n} = \frac{\delta}{\gamma},$$

et avec les relations bien connues

$$M_i N_{i-1} - M_{i-1} N_i = (-1)^i,$$
$$M_{i+1} = M_i k_{i+1} + M_{i-1}, \qquad N_{i+1} = N_i k_{i+1} + N_{i-1}.$$

Posons

$$z_1 = z + k_1 = S^{k_1}(z),$$
$$z_2 = -\frac{1}{z_1} = T(z_1) = S^{k_1}T(z),$$
$$z_3 = z_2 - k_2 = S^{-k_2}(z_2) = S^{k_1}TS^{-k_2}(z),$$
$$z_4 = -\frac{1}{z_3} = T(z_3) = S^{k_1}TS^{-k_2}T(z),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;$$

on peut démontrer, par induction, que la formule

$$z_{2i} = (-1)^i \frac{N_{i-1}z + M_{i-1}}{N_i z + M_i},$$

qui est vraie pour $i = 1$, subsiste pour toute autre valeur de i. Supposons-la vraie pour une certaine valeur de i; on a alors

$$\begin{aligned} z_{2i+1} &= z_{2i} + (-1)^i k_{i+1} \\ &= (-1)^i \frac{(N_i k_{i+1} + N_{i-1})z + M_i k_{i+1} + M_{i-1}}{N_i z + M_i} \\ &= (-1)^i \frac{N_{i+1}z + M_{i+1}}{N_i z + M_i}, \end{aligned}$$

et par suite

$$z_{2i+2} = -\frac{1}{z_{2i+1}} = (-1)^{i+1} \frac{N_i z + M_i}{N_{i+1}z + M_{i+1}},$$

qui revient à la formule (3), où l'on aurait remplacé i par $i+1$. On a donc

$$z_{2n} = -(-1)^n \frac{N_{n-1}z + M_{n-1}}{N_n z + M_n} = (-1)^n \frac{N_{n-1}z + M_{n-1}}{\gamma z + \delta}$$

avec

$$M_n N_{n-1} - M_{n-1} N_n = \delta N_{n-1} - \gamma M_{n-1} = (-1)^n$$

ou bien

$$\delta(-1)^n N_{n-1} - \gamma(-1)^n M_{n-1} = 1,$$

qui, en tenant compte de

$$\alpha\delta - \beta\gamma = 1,$$

devient

$$\delta[\alpha - (-1)^n N_{n-1}] = \gamma[\beta - (-1)^n M_{n-1}].$$

Et comme γ et δ sont premiers entre eux, on pourra écrire, λ désignant un certain nombre entier,

$$\alpha - (-1)^n N_{n-1} = \lambda\gamma, \qquad \beta - (-1)^n M_{n-1} = \lambda\delta,$$

en sorte que (4) devient

$$z_{2n} = \frac{(\alpha - \lambda\gamma)z + \beta - \lambda\delta}{\gamma z + \delta} = \frac{\alpha z + \beta}{\gamma z + \delta} - \lambda;$$

P peut donc s'écrire

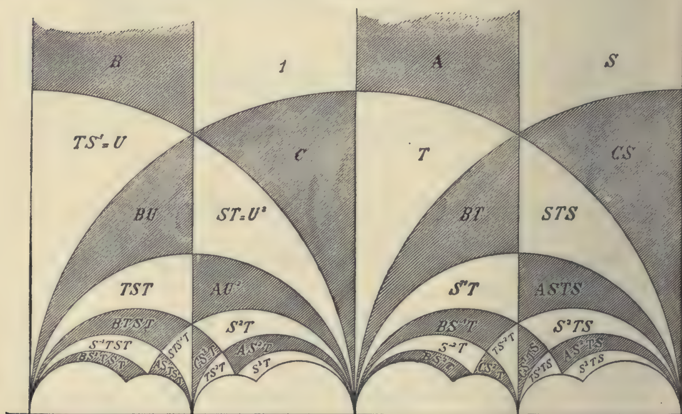
$$z' = z_{2n} + \lambda,$$

et l'on a finalement

$$P = S^{k_1} T S^{-k_2} T \ldots S^{(-1)^{n-1} k_n} T S^{\lambda}.$$

Donc le groupe correspondant à notre champ fondamental se compose de toutes les substitutions unitaires à coefficients entiers.

Fig. 27.



Pour des raisons que nous indiquerons plus loin, on le désigne sous le nom de *groupe modulaire* et on le représente généralement par Γ.

On peut considérer S et T comme les substitutions génératrices du groupe, en entendant par là que toute substitution du groupe

est un produit de puissances positives, nulles ou négatives de ces deux substitutions.

En se reportant aux développements donnés à propos des groupes finis, on pourra déterminer facilement les symboles correspondant à chacun des triangles du réseau. Disons seulement que, si P est le symbole d'un des triangles, les symboles des trois triangles adjacents seront

$$SP, \quad S^{-1}P, \quad TP.$$

88. *Le groupe modulaire ne comprend aucune substitution loxodromique* (nº 24).

Supposons qu'on ait donné aux coefficients des signes tels que

$$\alpha + \delta \geqq 0;$$

alors une substitution du groupe modulaire sera elliptique si

$$\alpha + \delta = 0 \qquad \text{ou} \qquad \alpha + \delta = 1,$$

parabolique si

$$\alpha + \delta = 2,$$

hyperbolique si

$$\alpha + \delta > 2.$$

Les substitutions pour lesquelles $\gamma = 0$ sont toutes paraboliques; en effet, dans ce cas, $\alpha\delta = 1$; par suite,

$$\alpha = \delta = \pm 1 \qquad \text{et} \qquad \alpha + \delta = \pm 2.$$

On peut se demander si le groupe modulaire comprend des substitutions d'ordre fini, c'est-à-dire (nº 33) des substitutions elliptiques.

Soit d'abord $\alpha + \delta = 0$. On a alors (nº 33)

$$\theta = \left[\frac{\alpha + \delta - \sqrt{(\alpha + \delta)^2 - 4}}{2}\right]^2 = -1 = e^{\pi i};$$

on a par suite une substitution d'ordre 2, dont les pôles sont

$$(1) \qquad \left.\begin{matrix} p \\ q \end{matrix}\right\} = \frac{\alpha - \delta \pm \sqrt{(\alpha + \delta)^2 - 4}}{2\gamma} = \frac{\alpha \pm i}{\gamma}.$$

Soit maintenant $\alpha + \delta = 1$. Alors

$$\theta = \left(\frac{1 - i\sqrt{3}}{2}\right)^2 = \frac{-1 - i\sqrt{3}}{2} = e^{\frac{4\pi i}{3}} = \rho^2,$$

d'où une substitution d'ordre 3, ayant pour pôles

$$(2) \qquad \begin{matrix} p \\ q \end{matrix} \Big\} = \left\{ \begin{matrix} \dfrac{\alpha+\rho}{\gamma}, \\ \dfrac{\alpha+\rho^2}{\gamma}. \end{matrix} \right.$$

Donc : *Les seules substitutions d'ordre fini du groupe modulaire sont, outre l'identité, celles pour lesquelles* $\alpha + \delta = 0$, $\alpha + \delta = \pm 1$; *elles sont respectivement d'ordres* 2 *et* 3.

Par exemple, la substitution

$$U = TS^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

est d'ordre 3, car $\alpha + \delta = 1$. Son inverse $ST = U^2$ est aussi d'ordre 3 (n° 5), ce qui donne entre S et T la relation simple

$$(3) \qquad STSTST = 1.$$

Les triangles 1, U, U^2 ont un sommet commun au point ρ.

89. Les formules (1) et (2) appellent quelques observations.

Des deux points p, q, un et un seul se trouve dans le demi-plan supérieur; supposons par exemple, ce qui est toujours permis, $\gamma > 0$; alors c'est le point $\dfrac{\alpha+i}{\gamma}$ qui se trouve dans le demi-plan supérieur. Cherchons quels sont ceux des points $\dfrac{\alpha+i}{\gamma}$ qui se trouvent dans le champ fondamental. Puisque tous les points du champ ont une ordonnée au moins égale à $\dfrac{\sqrt{3}}{2}$, on doit avoir $\gamma \leq \dfrac{2}{\sqrt{3}}$, ce qui donne comme unique solution $\gamma = 1$, et par suite $\dfrac{\alpha+i}{\gamma} = \alpha + i$. D'autre part, le seul point du champ fondamental dont l'abscisse soit un nombre entier est le point i; donc : *Les pôles des substitutions d'ordre* 2 *du groupe modulaire sont les points homologues du point* i.

Réciproquement p étant un point homologue de i, si Q et Q′ sont deux triangles ayant leur sommet en ce point, p est le pôle d'une substitution elliptique d'ordre 2 permettant de passer de Q à Q′, c'est-à-dire de la substitution $Q^{-1}Q'$. Donc : *Tout point homologue de* i *est pôle d'une substitution d'ordre* 2.

On voit de même, ρ et ρ^2 étant des quantités conjuguées, que un et un seul des points (2) appartient au demi-plan supérieur; par exemple $\frac{\alpha+\rho}{\gamma}$ si $\gamma > 0$.

Cherchons quels sont ceux des points $\frac{\alpha+\rho}{\gamma} = \frac{(2\alpha-1)+i\sqrt{3}}{2\gamma}$ situés dans le champ fondamental. On doit avoir tout d'abord

$$\frac{\sqrt{3}}{2\gamma} \geqq \frac{\sqrt{3}}{2} \qquad \text{c'est-à-dire } \gamma \leqq 1,$$

d'où nécessairement $\gamma = 1$, et

$$\frac{\alpha+\rho}{\gamma} = \frac{2\alpha-1}{2} + i\frac{\sqrt{3}}{2}.$$

Mais le seul point du champ fondamental ayant pour ordonnée $\frac{\sqrt{3}}{2}$ est le point ρ; donc $\alpha = 0$ et par suite

$$\frac{\alpha+\rho}{\gamma} = \rho.$$

Les pôles des substitutions d'ordre 3 du groupe modulaire sont les points homologues du point ρ.

On peut démontrer comme précédemment que réciproquement *tous les points homologues de ρ sont pôles d'une substitution d'ordre 3.*

90. Cela posé, examinons les conditions d'équivalence de deux substitutions elliptiques du groupe modulaire.

Soit d'abord P une substitution d'ordre 2. Son pôle situé dans le demi-plan supérieur est un point p homologue de i, c'est-à-dire un nœud du réseau, où se croisent quatre triangles; soit Q le symbole d'un des deux triangles blancs; l'autre triangle blanc se déduit du premier par une rotation d'angle π autour de p, pôle de P, et aura pour symbole QP. D'ailleurs, une rotation d'angle π autour du point i étant représentée par T, le produit TQ représente (n° 66) la même rotation que le produit QP. Ainsi

$$TQ = QP,$$

d'où

$$P = Q^{-1}TQ.$$

Donc :

Toute substitution d'ordre 2 du groupe modulaire est équivalente à la substitution T.

Et par suite :

Toutes les substitutions d'ordre 2 du groupe modulaire sont équivalentes entre elles.

Soit maintenant P une substitution elliptique d'ordre 3. Son pôle placé dans le demi-plan supérieur sera un point p homologue de ρ, donc un nœud du réseau autour duquel se croisent six triangles. Soit Q le symbole de l'un des trois triangles blancs situés autour de p; les deux autres triangles blancs seront QP et QP^2.

D'autre part, puisque p est le transformé de ρ par Q, les produits UQ et U^2Q représenteront les mêmes rotations que les produits QP et QP^2; par conséquent, on aura l'une ou l'autre des relations

$$UQ = QP, \qquad U^2Q = QP,$$

et, par suite,

$$P = Q^{-1}UQ \qquad \text{ou} \qquad P = Q^{-1}U^2Q.$$

Donc : *Toute substitution d'ordre 3 du groupe modulaire est équivalente ou à* U *ou à* U^2.

91. Traitons aussi le problème de l'équivalence pour les substitutions paraboliques.

Comme $\alpha + \delta = 2$, toute substitution parabolique du groupe modulaire pourra s'écrire

$$P = \begin{pmatrix} 1+\sigma & \beta \\ \gamma & 1-\sigma \end{pmatrix},$$

où β, γ, σ sont des nombres entiers positifs, nuls ou négatifs, liés par la relation

$$\beta\gamma + \sigma^2 = 0. \tag{1}$$

Soit λ le plus grand commun diviseur de β, γ, σ, pris avec le signe de β; posons

$$\beta = \lambda\beta', \qquad \gamma = \lambda\gamma', \qquad \sigma = \lambda\sigma';$$

on aura $\beta' > 0$. Soit de plus μ le plus grand commun diviseur de γ', σ', et posons

$$\gamma' = \mu\gamma'', \qquad \sigma' = \mu\nu;$$

μ sera premier avec β'. La relation (1) deviendra, en supprimant le facteur $\lambda^2\mu$,

$$\beta'\gamma'' + \mu\nu^2 = 0.$$

Mais, β' étant positif ou nul, μ premier avec β' et γ'' premier avec ν, la relation précédente donne

$$\beta' = \nu^2, \qquad \gamma'' = -\mu,$$

d'où

$$\beta = \lambda\nu^2, \qquad \gamma = -\lambda\mu^2, \qquad \sigma = \lambda\mu\nu,$$

en sorte que la substitution prend la forme

$$(2) \qquad P = \begin{pmatrix} 1+\lambda\mu\nu & \lambda\nu^2 \\ -\lambda\mu^2 & 1-\lambda\mu\nu \end{pmatrix}$$

et a pour pôle $-\frac{\mu}{\nu}$.

Nous avons déjà observé que μ est premier avec β'; comme $\beta' = \nu^2$, μ est premier avec ν. Il existe donc deux entiers μ' et ν' tels que

$$\nu\mu' - \mu\nu' = 1.$$

En posant alors

$$\begin{pmatrix} \mu' & \nu' \\ \mu & \nu \end{pmatrix} = Q,$$

on trouve facilement

$$QS^\lambda Q^{-1} = P.$$

Appelons *amplitude* de la substitution le nombre λ (de même signe que β) plus grand commun diviseur de $\alpha - 1$, β, γ. On peut dire que : *Toutes les substitutions d'amplitude λ sont équivalentes à S^λ et par suite équivalentes entre elles.*

Une substitution parabolique est déterminée si l'on se donne son pôle et son amplitude. En effet, si l'on connaît le pôle $-\frac{\mu}{\nu}$, μ et ν sont déterminés puisqu'ils sont premiers entre eux et de plus λ est connu. La formule (2) fournit alors la substitution cherchée.

L'amplitude a une signification géométrique très simple.

Considérons tout d'abord la substitution S^λ d'amplitude λ. On

passe d'un point à son homologue relativement à S^λ par une translation de grandeur λ parallèle à l'axe réel.

Cette translation a pour effet de changer l'un des bitriangles ayant un sommet au point ∞ en celui qui occupe le rang λ après lui. Posons

$$QS^\lambda Q^{-1} = P.$$

P est une substitution parabolique d'amplitude λ, ayant pour pôle un point c de l'axe réel, d'abscisse rationnelle. Aux faisceaux des bitriangles situés autour du point à l'infini, correspond dans le cas de la substitution P le faisceau des bitriangles entourant le point c. Donc, pour passer d'un point à son homologue dans P, il faut soumettre le plan à une déformation telle que l'un des triangles ayant un sommet en c vienne coïncider avec celui qui occupe le rang λ après lui.

92. Comme le réseau modulaire est symétrique par rapport à l'axe des quantités imaginaires, on obtiendra le groupe amplifié $\overline{\Gamma}$ en combinant Γ avec une réflexion A par rapport à cet axe. L'expression analytique de A est

$$z' = -\bar{z}.$$

Le symbole A appartient au triangle ombré symétrique du triangle blanc 1 par rapport au même axe. Il est clair que les triangles ombrés, symétriques du triangle 1 par rapport à ses deux autres côtés, ont pour symboles AS^{-1} et AT; les expressions analytiques correspondantes sont

$$z' = -\bar{z} - 1, \qquad z' = \frac{1}{\bar{z}}.$$

Nous poserons

$$(1) \qquad AS^{-1} = B,$$

$$(2) \qquad AT = C,$$

en sorte qu'on aura, pour les trois opérations génératrices du groupe $\overline{\Gamma}$,

$$A(z) = -\bar{z}, \qquad B(z) = -\bar{z} - 1, \qquad C(z) = \frac{1}{\bar{z}}.$$

Or A, B, C étant des réflexions, on a

$$(3) \qquad A^2 = B^2 = C^2 = 1.$$

Multiplions maintenant les deux membres de (1) à gauche par B, à droite par C, on aura $BAS^{-1}S = BBS$, ou bien

(4) $$BA = S;$$

multiplions au contraire à gauche par A, on aura $AAS^{-1} = AB$, ou

(5) $$AB = S^{-1}.$$

De la relation (2) il résulte ensuite

(6) $$AC = T,$$

et, en observant que l'inverse de AC est CA et que T est sa propre inverse,

(7) $$CA = T.$$

Enfin multiplions (1) à gauche par C, tenons compte de (7) et de la définition de U, on aura

(8) $$CB = U,$$

d'où

(9) $$BC = U^{-1} = U^2.$$

93. Passons maintenant à l'étude d'un sous-groupe très important du groupe Γ, que pour des raisons exposées un peu plus loin nous désignerons par Γ_6.

Considérons les substitutions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ du groupe modulaire pour lesquelles β et γ sont des nombres pairs. Ces substitutions forment un groupe. En effet, si nous posons

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix},$$

il résulte des formules (1) (n° 20) que, si $\beta, \gamma, \beta', \gamma'$ sont pairs, il en est de même de β'', γ''.

Le sous-groupe formé des substitutions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ du groupe modulaire, pour lesquelles β et γ sont pairs, est précisément le sous-groupe qu'on désigne par Γ_6.

Pour toutes les substitutions de Γ_6 les éléments α et δ sont impairs.

En effet, β et γ étant pairs, la relation

$$\alpha\delta - \beta\gamma = 1 \tag{1}$$

montre que le produit $\alpha\delta$ est impair; il en est donc de même de ses deux facteurs.

Le groupe Γ_6 *ne contient aucune substitution elliptique.*

Tout d'abord on ne peut avoir $\alpha + \delta = \pm 1$, puisque α et δ sont tous deux impairs. Si $\alpha + \delta$ était nul, on aurait, d'après (1),

$$\alpha^2 \equiv -1 \pmod 4,$$

ce qui est impossible.

Il suit de là (n° 87) que *les nœuds du réseau correspondant à* Γ_6 *sont situés sur l'axe réel.*

Démontrons que Γ_6 *est un sous-groupe invariant de* Γ.

Soient

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

une substitution quelconque de Γ_6 et

$$Q = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

une substitution quelconque de Γ. Posons

$$Q^{-1}PQ = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix};$$

on a (n° 68)

$$\left\{\begin{aligned} \alpha'' &= \alpha\alpha'\delta' - \beta\alpha'\gamma' + \gamma\beta'\delta' - \delta\beta'\gamma', \\ \beta'' &= -\alpha\alpha'\beta' + \beta\alpha'^2 - \gamma\beta'^2 + \delta\alpha'\beta', \\ \gamma'' &= \alpha\gamma'\delta' - \beta\gamma'^2 + \gamma\delta'^2 - \delta\gamma'\delta', \\ \delta'' &= -\alpha\beta'\gamma' + \beta\alpha'\gamma' - \gamma\beta'\delta' + \delta\alpha'\delta'. \end{aligned}\right. \tag{2}$$

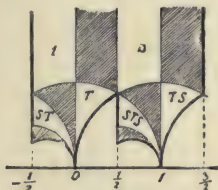
Comme β, γ et $\alpha - \delta$ sont pairs, β'' et γ'' le sont également, en sorte que $Q^{-1}PQ$ appartient à Γ_6.

94. Passons maintenant à la détermination du champ fondamental de Γ_6 en suivant la marche indiquée au n° 82. Considérons les trois bitriangles S, S^{-1}, T, adjacents au bitriangle 1.

Par rapport à Γ_6 aucun d'eux n'est homologue du bitriangle 1; mais S et S^{-1} sont homologues entre eux, car $S^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

appartient évidemment à Γ_6. Nous retiendrons donc pour notre champ fondamental les bitriangles 1, S, T. Les nouveaux bitriangles adjacents respectivement à S et T sont S^2, TS, ST, $S^{-1}T$; le premier est homologue de 1 et le dernier de ST, en sorte que nous ne garderons que TS et ST.

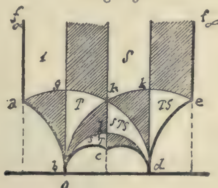
Fig. 28.



Les nouveaux bitriangles qui leur sont respectivement adjacents sont STS, $S^{-1}TS$, S^2T, TST. Le second et le quatrième sont homologues du premier [1], le troisième est homologue de T; nous ne garderons donc que STS. Des bitriangles adjacents à T, un seul est nouveau, S^2TS; mais il est homologue de TS. En définitive, le champ fondamental comprend les six bitriangles (*fig.* 28)

(1) 1, S, T, TS, ST, STS.

Fig. 29.



Le nombre des bitriangles ainsi obtenu justifie la notation Γ_6, que nous avons adoptée pour ce sous-groupe, dont l'indice est 6.

Modifions le champ fondamental, en remplaçant le bitriangle ST par son homologue $S^{-1}T$. On obtient un nouveau champ fonda-

---

(1) En effet, de la formule (3) ST ST ST = 1 (p. 128) on déduit

$$TST = S^{-1}TS^{-1} = S^{-2}.STS.S^{-2},$$

et S^{-2} appartient à Γ_6.

mental (*fig.* 29), symétrique par rapport à la droite $x = \frac{1}{2}$ et formé des six bitriangles

$$1, \quad S, \quad T, \quad TS, \quad ST, \quad STS.$$

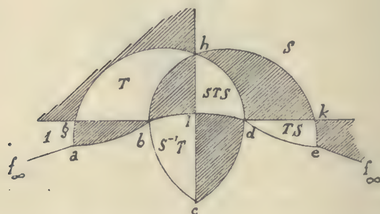
Désignons par Q_i les six substitutions précédentes ($i = 0, 1, 2, \ldots, 5$) et posons

$$\begin{aligned}
Q_0 &= \ 1 \ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & z' &= z, \\
Q_1 &= TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, & z' &= \frac{z-1}{z}, \\
Q_2 &= S^{-1}T = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, & z' &= -\frac{1}{z-1}, \\
Q_3 &= \ S \ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & z' &= z+1, \\
Q_4 &= \ T \ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & z' &= -\frac{1}{z}, \\
Q_5 &= STS = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, & z' &= \frac{z}{z+1};
\end{aligned}$$

on trouve immédiatement les relations suivantes :

$$Q_2 = Q_1^2, \qquad Q_4 = Q_1 Q_3 S^{-2},$$
$$Q_5 = S^2 Q_1^2 Q_3, \qquad Q_1^3 = 1, \qquad Q_3^2 = S^2.$$

Fig. 30.



Si nous introduisons la notation $\simeq$ pour désigner *l'égalité aux substitutions près de* Γ_6, nous pourrons écrire

$$Q_2 \simeq Q_1^2, \qquad Q_4 \simeq Q_1 Q_3, \qquad Q_5 \simeq Q_1^2 Q_3, \qquad Q_1^3 \simeq 1, \qquad Q_3^2 \simeq 1;$$

on peut dire alors que le groupe des transformations en elle-même

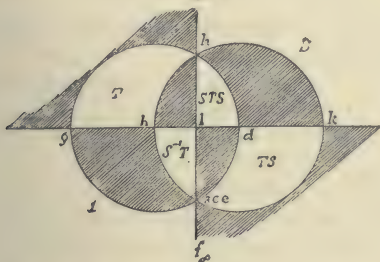
de la surface fermée à laquelle se ramène le champ fondamental est le suivant :

$$1, \quad Q_1, \quad Q_1^2, \quad Q_3, \quad Q_1 Q_3, \quad Q_1^2 Q_3.$$

C'est évidemment (n° 85) un groupe diédrique ($m = 3$).

On parvient au même résultat par voie intuitive en montrant comment le champ fondamental de Γ_6 peut être ramené par déformation continue à une sphère contenant un réseau de 12 triangles ($m = 3$). Les figures 30 et 31 représentent une phase intermédiaire et la phase finale de cette déformation.

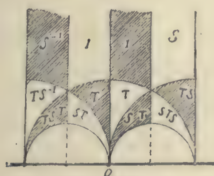
Fig. 31.



La figure 31 qui est identique à la figure 23 n'est autre qu'un réseau diédrique projeté stéréographiquement sur l'équateur, en prenant l'un des nœuds comme point de vue.

95. Effectuons sur la figure 29 les modifications permises suivantes :

Fig. 32.



Remplaçons les triangles blancs TS, $S^{-1}T$ par leurs homologues blancs TS^{-1} et ST. Remplaçons de même les triangles ombrés S, STS par leurs homologues ombrés S^{-1}, TST.

Nous obtenons ainsi Γ_6 un nouveau champ fondamental (*fig.* 32) symétrique par rapport à l'axe imaginaire ([1]).

Cela montre que le groupe Γ_6 peut être amplifié par la réflexion A. On peut prendre comme champ fondamental du groupe amplifié $\overline{\Gamma_6}$ une des deux moitiés en lesquelles le champ fondamental de Γ_6 est divisé par l'axe imaginaire, par exemple celle de gauche. Ce champ n'est autre qu'un triangle à côtés rectilignes ou circulaires, ayant ses trois angles nuls et ses sommets aux points $0, -1, \infty$. Donc le groupe Γ_6 a pour image un réseau triangulaire dans lequel

$$\nu_1 = \nu_2 = \nu_3 = \infty,$$

qui appartient par conséquent au type (c) du n° 76, et admet l'axe réel pour cercle de symétrie.

Les opérations génératrices de $\overline{\Gamma_6}$ sont les trois réflexions par rapport aux trois côtés du triangle $(0, -1, \infty)$. Les réflexions par rapport aux deux côtés rectilignes sont

$$z' = A'(z) = -\bar{z}, \qquad z' = B'(z) = -\bar{z} - 2.$$

Pour trouver l'expression analytique de la troisième, utilisons les formules du n° 40. Le cercle de symétrie a pour centre le point $-\frac{1}{2}$ et pour rayon $\frac{1}{2}$. Par suite

$$\frac{\alpha}{\gamma} = -\frac{1}{2}, \qquad \frac{\alpha_1^2 + \alpha_2^2 + \beta\gamma}{\gamma^2} = \frac{1}{4}.$$

Prenons $\gamma = -2$, d'où

$$\alpha = +1, \qquad \alpha_1 = +1, \qquad \alpha_2 = 0, \qquad \beta = 0;$$

mais d'autre part $\delta = -\bar{\alpha}$, d'où $\delta = -1$. En sorte que la réflexion cherchée est

$$z' = C'(z) = \frac{\bar{z}}{-2\bar{z} - 1}.$$

Or, comme chacune des substitutions de Γ_6 est le produit d'un nombre pair de facteurs A', B', C' et que

$$A' = B'^2 = C'^2 = 1,$$

([1]) Ce champ diffère des deux précédents (*fig.* 28 et 29) en ce qu'il ne comprend pas six bitriangles.

on pourra prendre pour substitutions génératrices de Γ_6 les trois produits

$$B'A' = S', \qquad C'A' = T', \qquad C'B' = U',$$

et l'on trouvera

$$S' = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = S^2, \qquad z' = z + 2,$$

$$T' = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = TS^{-2}T, \qquad z' = \frac{z}{2z+1},$$

$$U' = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} = T'S'^{-1} \qquad z' = \frac{3z+2}{-2z-1}.$$

Enfin, puisque le champ fondamental de Γ_6 est symétrique par rapport à l'axe imaginaire, on en déduit aussi (note page 114) que Γ_6 *est un sous-groupe invariant de* $\overline{\Gamma}$.

96. Revenons au groupe diédrique du nº **94**, que nous désignerons par G_6, et déterminons ses sous-groupes; à chacun d'eux correspondra un sous-groupe de Γ contenant Γ_6.

Les sous-groupes de G_6 sont :

Un groupe cyclique d'ordre 3, soit G_3,

$$1, \quad Q_1, \quad Q_1^2,$$

qui, étant unique, est nécessairement invariant;

Trois groupes cycliques d'ordre 2, équivalents entre eux,

$$1, \quad Q_3; \quad 1, \quad Q_1 Q_3; \quad 1, \quad Q_1^2 Q_3.$$

Aux sous-groupes précédents correspondront dans Γ un sous-groupe invariant Γ_2 d'indice $\frac{6}{3} = 2$, et trois sous-groupes équivalents Γ_3, Γ'_3, Γ''_3 d'indice $\frac{6}{2} = 3$.

Construisons leurs champs fondamentaux.

Le sous-groupe Γ_2 comprend toutes les substitutions de Γ égales à l'une ou l'autre des substitutions

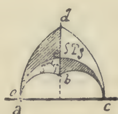
$$(1) \qquad 1, \quad TS, \quad S^{-1}T,$$

et cela aux substitutions près de Γ_6. Son champ fondamental est donc formé de deux des six bitriangles, constituant le champ fondamental de Γ_6. L'un d'entre eux peut être choisi arbitrairement;

quant à l'autre, il est adjacent au premier et soumis à la condition de ne pas avoir un symbole égal à celui du premier, aux substitutions (1) près; en d'autres termes, il ne doit pas être homologue du premier dans Γ_2.

Choisissons comme premier bitriangle $S^{-1}T$, c'est-à-dire Q_2. Le bitriangle adjacent $STS = Q_5$ ne lui est pas homologue dans Γ_2, puisque aucun des produits de substitutions (1) par STS n'est égal à $S^{-1}T$. Nous pouvons donc prendre pour champ fondamental (*fig.* 33) de Γ_2 l'ensemble des bitriangles $S^{-1}T = Q_2$ et $STS = Q_5$.

Fig. 33.



On peut prendre encore le champ formé des deux bitriangles $1 = Q_0$ et $T = Q_4$ (*fig.* 34). Ce champ étant symétrique par rapport à l'axe imaginaire, Γ_2 est (note p. 114) *un sous-groupe invariant de* $\overline{\Gamma}$.

Reprenons le champ représenté par la figure 33. Comme $S^{-1}T$ et TS sont homologues dans Γ_2, il en est de même de $S^{-1}T$ et du triangle S^2TS adjacent à STS le long de bc. Donc les côtés ad et cd sont homologues et aussi ab, cb.

Fig. 34.

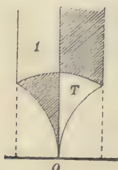
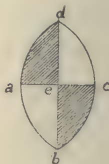


Fig. 35.



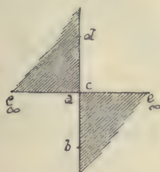
Déformons le champ comme l'indique la figure 35, appliquons-le sur une sphère, et pour fixer les idées donnons à b et d deux positions diamétralement opposées. Alors bed, bad, bcd sont disposés suivant des méridiens et aec suivant l'équateur. Fixons le méridien bed, et étendons notre surface sur la sphère jusqu'à ce

qu'elle la recouvre complètement; dans ces conditions *bad* et *bcd* seront confondus.

Nous aurons alors sur la sphère un réseau qui, projeté stéréographiquement, avec *e* pour point de vue, sera représenté par la figure 36.

Procédons d'une façon analogue pour les groupes Γ_3, Γ'_3, Γ''_3.

Fig. 36.



Le groupe Γ_3 comprend toutes les substitutions de Γ égales, aux substitutions près de Γ_6, à l'une ou l'autre des deux substitutions.

(2) 1, S.

Pour former son champ fondamental, partons du bitriangle 1. Les deux bitriangles adjacents sont S et T. S qui est homologue de 1 dans Γ_3 doit être laissé de côté; au contraire nous devons garder T. On peut prendre comme troisième bitriangle $S^{-1}T$ qui, dans Γ_3, n'est homologue, ni de 1, ni de T; on obtient ainsi le champ représenté par la figure 37.

Fig. 37.

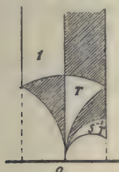
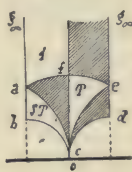


Fig. 38.

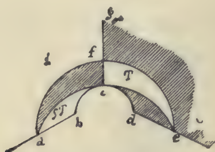


Ce champ peut être modifié de façon à devenir symétrique par rapport à l'axe imaginaire : on remplacera le triangle blanc $S^{-1}T$ par le triangle blanc ST qui est son homologue dans Γ_6 et par suite dans Γ_3.

Puisque, dans Γ_3, ST est homologue de STS et de $S^{-1}T$ et que I

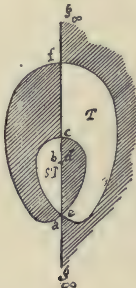
est homologue de S, les côtés ab, de; bc, cd; ag, eg sont des couples respectivement homologues. Déformons le champ comme l'indiquent les figures 39 et 40; nous obtenons un plan ou une

Fig. 39.



sphère partagés en six champs. Il n'est pas inutile d'observer que le réseau de la figure 40 n'est pas régulier; cela tient (n° 83) à ce que

Fig. 40.



Γ_3 n'est pas un sous-groupe invariant. Ainsi, tandis que b et f sont tous deux des nœuds de première espèce, en b et f se croisent respectivement deux et quatre triangles. De même c et g sont tous deux des nœuds de troisième espèce, où se croisent respectivement quatre et deux triangles.

Passons au groupe Γ_3'. Au lieu des substitutions (2) nous devons considérer les substitutions

$$1, \quad T.$$

Les considérations habituelles montrent qu'on peut former le champ fondamental de Γ_3' avec les bitriangles 1, S, TS. Remplaçons ensuite le triangle ombré S et le triangle blanc TS par le triangle ombré S^{-1} et le triangle blanc TS^{-1} qui leur sont respectivement

homologues; on obtient (*fig.* 42) un champ symétrique par rapport à l'axe imaginaire.

Fig. 41.

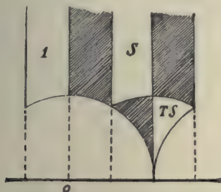
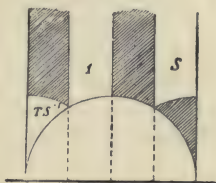


Fig. 42.



Enfin, pour le groupe Γ''_3, on considérera les substitutions

$$1, \quad STS.$$

Le champ fondamental (*fig.* 43) peut être constitué par les bitriangles 1, S, T.

Fig. 43.

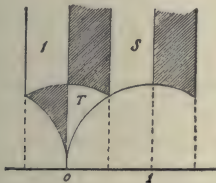
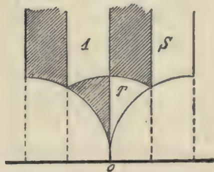


Fig. 44.



On le rend symétrique par rapport à l'axe imaginaire (*fig.* 44) en remplaçant le triangle ombré S par son homologue, le triangle ombré S^{-1}.

En ramenant les champs fondamentaux de Γ'_3, Γ''_3 à des surfaces fermées, on obtiendra deux figures qui, par suite de l'équivalence des trois sous-groupes Γ_3, Γ'_3, Γ''_3, ne différeront pas essentiellement de la figure relative à Γ_3.

97. Pour obtenir d'autres sous-groupes du groupe modulaire, nous utiliserons le principe suivant, dit PRINCIPE D'EXISTENCE DES SOUS-GROUPES (1) :

(1) On pourrait établir un principe analogue pour des groupes plus généraux que le groupe modulaire; mais cela ne nous serait d'aucune utilité.

Soient une surface fermée C_s et sur cette surface un réseau de 2s triangles. Supposons qu'on puisse diviser les nœuds du réseau en trois espèces : ceux de première espèce où se croisent 2 ou 4 triangles; ceux de deuxième espèce où se croisent 2 ou 6 triangles, et enfin ceux de troisième espèce où se croisent un nombre pair de triangles. Supposons de plus que les trois sommets de chaque triangle appartiennent respectivement à ces trois espèces. Il existe alors un système de sous-groupes de Γ *d'indice s et équivalents.*

Indiquons rapidement la démonstration de ce principe, laquelle résultera encore plus clairement des applications ultérieures.

Supposons les triangles de la surface C_s alternativement blancs et ombrés; prenons l'un quelconque des triangles blancs et faisons-lui correspondre le triangle blanc 1 du réseau modulaire. Établissons une correspondance analogue pour les triangles adjacents, et cela de façon que les nœuds de première, deuxième et troisième espèce correspondent respectivement aux nœuds de même espèce du réseau modulaire. Nous obtiendrons ainsi dans le plan une figure connexe D_s formée de bitriangles. A chaque côté de C_s correspondra dans D_s ou un côté intérieur, ou un couple de côtés situés sur le contour. Soient l, l' un de ces couples, h le côté correspondant de C_s, b le triangle de D_s auquel appartient l, a le triangle correspondant de C_s, b' le triangle du réseau modulaire extérieur à D_s, dont l' est un côté. Regardant comme correspondant au triangle a de C_s, non plus le triangle b, mais le triangle b' du réseau modulaire, et procédant comme plus haut, nous pourrons construire une autre figure connexe D'_s composée de s bitriangles du réseau modulaire, et qu'on peut considérer également comme correspondant à C_s. En continuant de la sorte, on pourra trouver une infinité de figures du réseau modulaire, adjacentes entre elles, qui toutes pourront être considérées comme correspondantes à C_s; et, en vertu des hypothèses faites sur le nombre des triangles se croisant en chaque nœud de C_s, aucune partie du plan ne sera recouverte plus d'une fois.

Maintenant, comme on l'a vu, le champ D_s peut être pris pour champ fondamental d'un sous-groupe de Γ d'indice s, dont nous savons trouver les substitutions génératrices ; et C_s n'est autre

que la surface obtenue en déformant D_s de façon à amener la coïncidence des côtés homologues. De plus, si nous choisissons autrement le triangle de C_s, correspondant au triangle 1 du réseau modulaire, nous obtiendrons en général un champ différent de D_s, et un sous-groupe différent du sous-groupe précédent. Mais ces deux sous-groupes seront équivalents, parce que leurs champs fondamentaux peuvent être ramenés à une même surface fermée.

Ce principe permet de construire, à l'aide d'un nombre fini d'opérations, tous les sous-groupes de Γ, d'indice fini s donné; on forme tous les groupements connexes comprenant le bitriangle 1 et constitués par s bitriangles du réseau modulaire; on établit arbitrairement pour chacun de ces champs une correspondance entre les côtés extérieurs de la figure résultante, et on le ramène à une surface fermée, en amenant la coïncidence des côtés opposés. Si cette surface fermée satisfait aux conditions du principe d'existence, elle définit un système de sous-groupes équivalents d'indice s. Il est bien évident que cette façon de procéder donne tous les sous-groupes d'indice s du groupe modulaire.

98. Occupons-nous en particulier du cas où le réseau tracé sur la surface fermée C_s est régulier. Soient (n° 86) $2n_1$, $2n_2$, $2n_3$ les nombres de triangles se croisant aux nœuds de première, deuxième et troisième espèce, et désignons le réseau par le symbole (n_1, n_2, n_3). Pour que les conditions du principe d'existence soient satisfaites, n_1 doit avoir une des valeurs 1 ou 2 et n_2 une des valeurs 2 ou 3. Cherchons les cas les plus simples en utilisant (n° 86) la formule

$$(1) \qquad p = 1 - s + \sum_{i=1}^{3} \frac{s}{n_i} \frac{n_i - 1}{2},$$

en se rappelant que p ne peut être négatif, et que s doit être multiple de n_1, n_2, n_3.

Pour simplifier, écrivons r à la place de n_3.

Voici les quatre types correspondants :

$$(1, 1, r); \quad (2, 1, r); \quad (1, 3, r); \quad (2, 3, r).$$

Pour le type (1, 1, r), la formule (1) donne

$$p = 1 - s + \frac{s}{r}\,\frac{r-1}{2} = 1 - s\,\frac{r+1}{2r} < 1 - \frac{s}{2};$$

d'où $s < 2$, par suite $s = 1$ et $p = 0$. Dans le cas actuel, on a le symbole unique (1, 1, 1); le réseau se compose d'un seul couple de triangles et le sous-groupe correspondant est le groupe modulaire lui-même.

Pour le second type (2, 1, r)

$$p = 1 - s + \frac{s}{4} + \frac{s}{r}\,\frac{r-1}{2} = 1 - \frac{s}{4} - \frac{s}{2r} < 1 - \frac{s}{4},$$

d'où $p = 0$, $s < 4$, et, puisque s doit être multiple de $n_1 = 2$, on a $s = 2$ et enfin $r = 2$. Le symbole correspondant est donc (2, 1, 2); le réseau est celui de la figure 35; les quatre triangles se croisent tous au point e de première espèce et au point d de troisième espèce, tandis que les deux autres se croisent en chacun des points de deuxième espèce b, d.

Le sous-groupe correspondant est donc le groupe Γ_2, déjà étudié.

Pour le troisième type, on a

$$p = 1 - s + \frac{s}{3} + \frac{s}{r}\,\frac{r-1}{2} = 1 - \frac{s}{6} - \frac{s}{2r} < 1 - \frac{s}{6};$$

d'où $p = 0$, $s < 6$ et, comme s doit être multiple de $n_2 = 3$, $s = 3$. Il en résulte $r = 3$, d'où le symbole (1, 3, 3). Nous ne nous occuperons pas du groupe correspondant, qui ne présente pour nous aucun intérêt particulier : il a pour champ fondamental les bitriangles 1, S, S^2.

Arrivons enfin au quatrième type. On a

$$p = 1 - s + \frac{s}{4} + \frac{s}{3} + \frac{s}{r}\,\frac{r-1}{2} = 1 + \frac{s}{12} - \frac{s}{2r},$$

d'où

$$s = \frac{12\,r(p-1)}{r-6}. \qquad (2)$$

Ici il y a un nombre infini de solutions; nous ne considérerons que les plus simples et nous désignerons par $\Gamma_{[r]}$ le sous-groupe correspondant au réseau (2, 3, r).

Soit d'abord $p = 0$; alors

$$s = \frac{12r}{6 - r};$$

on doit avoir $r < 6$, et, puisque r est un diviseur de s, le quotient $\frac{12}{6-r}$ doit être entier. Les valeurs possibles de r sont donc 2, 3, 4, 5, auxquelles correspondent respectivement les valeurs $s = 6$, 12, 24, 60. On obtient alors les réseaux suivants :

(2, 3, 2), c'est le réseau diédrique pour $m = 3$; il donne lieu, comme on l'a déjà vu, au sous-groupe Γ_6, que nous pouvons maintenant désigner aussi par la notation $\Gamma_{[2]}$;

(2, 3, 3), c'est le réseau tétraédrique qui, d'après le principe d'existence, donne lieu à un sous-groupe invariant $\Gamma_{[3]}$ d'indice 12;

(2, 3, 4), c'est le réseau octaédrique qui donne lieu à un sous-groupe invariant $\Gamma_{[4]}$ d'indice 24;

(2, 3, 5), c'est le réseau icosaédrique qui donne lieu à un sous-groupe invariant $\Gamma_{[5]}$ d'indice 60.

Supposons maintenant $p = 1$. D'après (2), $r = 6$, quel que soit s, d'où le symbole (2, 3, 6). On peut le vérifier en prenant une partie finie quelconque du réseau (*fig.* 17) et la faisant correspondre à une portion du réseau modulaire de façon que les angles $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{6}$ de la première correspondent aux angles $\frac{\pi}{2}, \frac{\pi}{3}, 0$ de la seconde.

Faisons enfin $p = 2$. La formule (2) devient

$$s = \frac{12r}{r - 6};$$

$r - 6$ doit être diviseur de 12, d'où $r = 7$, 8, 9, 10, 12, 18 et $s = 84$, 48, 36, 30, 24, 18 : on a donc les symboles suivants :

$$\begin{array}{ll}
(2, 3, 7), & s = 84, \\
(2, 3, 8), & s = 48, \\
(2, 3, 9), & s = 36, \\
(2, 3, 10), & s = 30, \\
(2, 3, 12), & s = 24, \\
(2, 3, 18), & s = 18.
\end{array}$$

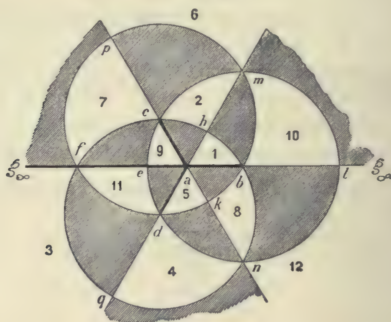
Il est à peine besoin de rappeler que tous les symboles trouvés

représentent des réseaux *arithmétiquement possibles;* il resterait à examiner si, dans chaque cas, il existe effectivement un réseau régulier répondant aux données, et s'il en est ainsi on pourra affirmer, en vertu du principe d'existence, qu'il existe dans Γ un sous-groupe correspondant.

99. Comme on vient de le voir, le réseau diédrique pour $m = 3$ et les autres réseaux polyédriques donnent lieu à autant de sous-groupes de Γ. Nous ne donnerons la construction effective du sous-groupe que pour le réseau tétraédrique, nous bornant pour les autres cas à renvoyer le lecteur à l'Ouvrage classique de Klein-Fricke.

Reprenons la figure 11, où pour simplifier nous désignerons les triangles blancs non plus par les symboles qui les caractérisent,

Fig 45.

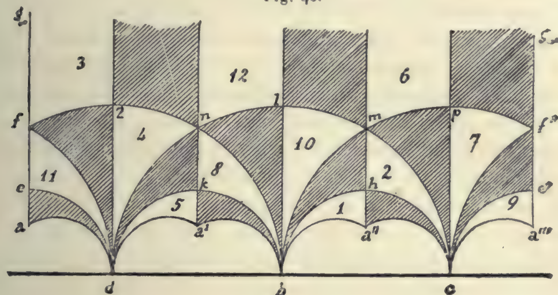


mais par des numéros d'ordre allant de 1 à 12. Fendons la sphère suivant les lignes formées de gros traits et déformons convenablement le réseau. On pourra l'amener à coïncider avec une portion du réseau modulaire, ainsi que l'indique la figure 46. Cette partie du réseau est le champ fondamental du sous-groupe invariant $\Gamma_{(3)}$ ou Γ_{12} de Γ.

Les opérations génératrices du groupe sont celles qui transforment l'un dans l'autre les bords correspondants des coupures, c'est-à-dire, ici, celles qui changent ag, $a'd$, $a''b$, $a'''c$ respectivement en $a'''g$, ad, $a'b$, $a''c$. Ce sont, comme on le voit sur la figure,

quatre substitutions paraboliques d'amplitude 3 dont les pôles sont respectivement les points ∞, -1, 0, $+1$.

Fig. 46.



Faisons dans la formule (2) du n° 91 successivement

$$\begin{array}{lll} \lambda = 3, & \mu = 0, & \nu = 1, \\ \lambda = 3, & \mu = 1, & \nu = 1, \\ \lambda = 3, & \mu = 1, & \nu = 0, \\ \lambda = 3, & \mu = 1, & \nu = -1; \end{array}$$

on obtient les quatre substitutions

$$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 3 \\ -3 & -2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}, \quad \begin{pmatrix} -2 & 3 \\ -3 & 4 \end{pmatrix}.$$

100. Soit un réseau régulier $(2, 3, n)$ de $2s$ triangles situé sur une surface fermée C_s. Si l'on fend la surface suivant certaines lignes et qu'on la déforme ensuite convenablement, on pourra l'amener à coïncider avec un ensemble connexe D_s de $2s$ triangles du réseau modulaire. Le réseau modulaire est ainsi décomposé en une infinité de champs homologues de D_s, dans le groupe $\Gamma_{[n]}$ défini par le réseau primitif.

Puisque, en un nœud de première espèce aussi bien de C_s que du réseau modulaire se trouvent quatre triangles, à une ligne fermée de C_s, tracée autour d'un nœud de première espèce, correspondra sur le plan une ligne fermée analogue; il en est de même pour les nœuds de deuxième espèce. Au contraire, tandis que sur la surface C_s en un nœud de troisième espèce se croisent

$2n$ triangles, au nœud correspondant du réseau modulaire il s'en trouve une infinité, et, par suite, à une ligne fermée de C_s entourant un nœud de troisième espèce, correspondra dans le plan une ligne ouverte allant d'un point à un de ses homologues, traversant n triangles ayant un sommet commun au nœud de troisième espèce correspondant à celui de C_s. Et puisque toute ligne fermée de C_s équivaut à un ensemble de lignes fermées entourant chacune un seul nœud, on peut passer d'un point du plan à un quelconque de ses homologues dans $\Gamma_{[n]}$ au moyen d'une succession de mouvements analogues au précédent.

En se reportant aux développements indiqués au n° 91, on peut exprimer ce fait en disant que *toute substitution de* $\Gamma_{[n]}$ *est un produit de substitutions paraboliques d'amplitude* n.

Or de telles substitutions sont équivalentes entre elles (n° 91), et comme d'autre part le sous-groupe $\Gamma_{[n]}$ est invariant, c'est-à-dire n'a d'autre équivalent que lui-même, $\Gamma_{[n]}$ *contient toutes les substitutions paraboliques d'amplitude* n *du groupe modulaire*.

Le groupe Γ se réduit, aux substitutions près de $\Gamma_{[n]}$, à un groupe fini $G_{[n]}$ d'ordre s, qui lui est isomorphe; à la substitution identique de $G_{[n]}$ correspond dans Γ précisément le sous-groupe $\Gamma_{[n]}$, et à chaque sous-groupe de $G_{[n]}$ correspond un sous-groupe de Γ contenant $\Gamma_{[n]}$. Le groupe $G_{[n]}$ peut aussi être considéré comme le groupe des transformations en elle-même de la surface C_s.

101. Un sous-groupe important de Γ admettant à son tour $\Gamma'_{[n]}$ comme sous-groupe est le groupe formé par toutes les substitutions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ de Γ pour lesquelles

$$(1) \qquad \alpha \equiv \delta \equiv 1, \qquad \beta \equiv \gamma \equiv 0 \qquad (\text{mod}\, n);$$

nous le désignerons provisoirement par $\Gamma_{\{n\}}$. Ces substitutions forment évidemment un groupe. En effet, de

$$\alpha \equiv \delta \equiv 1, \quad \beta \equiv \gamma \equiv 0, \quad \alpha' \equiv \delta' \equiv 1, \quad \beta' \equiv \gamma' \equiv 0 \quad (\text{mod}\, n),$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha'\alpha + \beta'\gamma & \alpha'\beta + \beta'\delta \\ \gamma'\alpha + \delta'\gamma & \gamma'\beta + \delta'\delta \end{pmatrix} = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix},$$

il suit

$$\alpha'' \equiv \delta'' \equiv 1, \qquad \beta'' \equiv \gamma'' \equiv 0 \qquad (\text{mod}\, n).$$

On voit ensuite que $\Gamma_{\{n\}}$ est un sous-groupe de $\Gamma_{(n)}$; cela résulte (n° 91) de ce que toute substitution parabolique d'amplitude n satisfait aux congruences (1), par suite appartient à $\Gamma_{\{n\}}$, et que chaque substitution de $\Gamma_{\{n\}}$ est un produit de substitutions paraboliques d'amplitude n.

Le sous-groupe $\Gamma_{\{n\}}$ *est invariant.*

Soient $P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une substitution quelconque de $\Gamma_{\{n\}}$ et $Q = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ une substitution quelconque de Γ. Si l'on pose

$$Q^{-1}PQ = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix},$$

les expressions de α'', β'', γ'', δ'' sont données par les formules (2) (n° 93), qu'on peut écrire en tenant compte de $\alpha'\delta' - \beta'\gamma' = 1$:

$$\begin{aligned}
\alpha'' &= \quad (\alpha - \delta)\alpha'\delta' - \beta\alpha'\gamma' + \gamma\beta'\delta' + \delta,\\
\beta'' &= -(\alpha - \delta)\alpha'\beta' + \beta\alpha'^2 \quad - \gamma\beta'^2,\\
\gamma'' &= \quad (\alpha - \delta)\gamma'\delta' - \beta\gamma'^2 \quad + \gamma\delta'^2,\\
\delta'' &= -(\alpha - \delta)\alpha'\delta' + \beta\alpha'\gamma' - \gamma\beta'\delta' + \alpha.
\end{aligned}$$

Supposons de plus que α, β, γ, δ satisfassent aux congruences (1); on aura

$$\alpha'' \equiv \delta'' \equiv 1, \qquad \beta'' \equiv \gamma'' \equiv 0 \qquad (\bmod n),$$

en sorte que $Q^{-1}PQ$ appartient à $\Gamma_{\{n\}}$.

On peut ajouter que $\Gamma_{\{n\}}$ *est aussi un sous-groupe invariant de* $\overline{\Gamma}$; en effet,

$$APA = \begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix},$$

$$BPB = \begin{pmatrix} \alpha + \gamma & \alpha - \beta + \gamma - \delta \\ -\gamma & \delta - \gamma \end{pmatrix}, \qquad CPC = \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix};$$

et l'on voit que ces substitutions appartiennent à $\Gamma_{\{n\}}$, en même temps que P.

102. Pour établir que $\Gamma_{\{n\}}$ est un sous-groupe invariant d'indice fini, et déterminer cet indice, il convient de faire tout d'abord quelques remarques.

Nous dirons que deux substitutions

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad P' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

sont *congrues* suivant le module n, et nous écrirons

$$P \equiv P' \pmod{n}$$

si l'on a

$$(1) \qquad \alpha' \equiv \alpha, \quad \beta' \equiv \beta, \quad \gamma' \equiv \gamma, \quad \delta' \equiv \delta \pmod{n},$$

ou bien

$$(2) \qquad \alpha' \equiv -\alpha. \quad \beta' \equiv -\beta, \quad \gamma' \equiv -\gamma, \quad \delta' \equiv -\delta \pmod{n}.$$

Toutes les substitutions de $\Gamma_{\{n\}}$ *et celles-là seulement satisfont à la congruence*

$$P \equiv 1 \pmod{n} \quad (^1).$$

Si $\Gamma_{\{n\}}$ *contient* P, *il contient aussi* P^{-1}.

Si $P \equiv 1$,

$$PP' \equiv P'P \equiv P'.$$

En effet, si $\alpha, \beta, \gamma, \delta$ satisfont aux congruences (1) du n° 101, on a, quels que soient $\alpha', \beta', \gamma', \delta'$,

$$\begin{aligned} \alpha'\alpha + \beta'\gamma &\equiv \alpha'\alpha + \gamma'\beta \equiv \alpha', \\ \alpha'\beta + \beta'\delta &\equiv \beta'\alpha + \delta'\beta \equiv \beta', \\ \gamma'\alpha + \delta'\gamma &\equiv \alpha'\gamma + \gamma'\delta \equiv \gamma', \\ \gamma'\beta + \delta'\delta &\equiv \beta'\gamma + \delta'\delta \equiv \delta'. \end{aligned}$$

Si $P \equiv P'$,

$$PP'^{-1} \equiv P'^{-1}P \equiv 1$$

et réciproquement.

On a

$$P'^{-1} = \begin{pmatrix} \delta' & -\beta' \\ -\gamma' & \alpha' \end{pmatrix},$$

---

(1) Il est à peine utile de faire observer que 1 représente ici la substitution identique $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Dorénavant, pour simplifier l'écriture, nous supprimerons dans les congruences la notation *mod n*, quand cela ne donnera lieu à aucune équivoque.

d'où

$$PP'^{-1} = \begin{pmatrix} \delta'\alpha - \beta'\gamma & \delta'\beta - \beta'\delta \\ -\gamma'\alpha + \alpha'\gamma & -\gamma'\beta + \alpha'\delta \end{pmatrix},$$

$$P'^{-1}P = \begin{pmatrix} \delta'\alpha - \gamma'\beta & -\beta'\alpha + \alpha'\beta \\ \delta'\gamma - \gamma'\delta & -\beta'\gamma + \alpha'\delta \end{pmatrix}.$$

Supposons maintenant

$$\alpha' \equiv \pm\alpha, \qquad \beta' \equiv \pm\beta, \qquad \gamma' \equiv \pm\gamma, \qquad \delta' \equiv \pm\delta,$$

où le signe doit être le même dans ces quatre formules; on a

$$\begin{aligned} \delta'\alpha - \beta'\gamma &\equiv \pm(\alpha\delta - \beta\gamma) \equiv \pm 1, \\ \delta'\beta - \beta'\delta &\equiv 0, \\ -\gamma'\alpha + \alpha'\gamma &\equiv 0, \\ -\gamma'\beta + \alpha'\delta &\equiv \pm(\alpha\delta - \beta\gamma) = \pm 1, \\ \delta'\alpha - \gamma'\beta &\equiv \pm(\alpha\delta - \beta\gamma) = \pm 1, \\ -\beta'\alpha + \alpha'\beta &\equiv 0, \\ \delta'\gamma - \gamma'\delta &\equiv 0, \\ -\beta'\gamma + \alpha'\delta &\equiv \pm(\alpha\delta - \beta\gamma) = \pm 1. \end{aligned}$$

Réciproquement, si l'on suppose

$$\begin{aligned} \delta'\alpha - \beta'\gamma &\equiv -\gamma'\beta + \alpha'\delta \equiv 1, \\ \delta'\beta - \beta'\delta &\equiv -\gamma'\alpha + \alpha'\gamma \equiv 0 \end{aligned}$$

et si l'on tient compte de

$$\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma = 1,$$

on a

$$\begin{aligned} \alpha(\delta - \gamma') - \gamma(\beta - \beta') &\equiv 0, \\ \beta(\delta - \delta') - \delta(\beta - \beta') &\equiv 0, \\ -\beta(\gamma - \gamma') + \delta(\alpha - \alpha') &\equiv 0, \\ -\alpha(\gamma - \gamma') + \gamma(\alpha - \alpha') &\equiv 0. \end{aligned}$$

Multiplions la première de ces relations par δ et la deuxième par $-\gamma$ et ajoutons-les, puis multiplions la première par β et la deuxième par $-\alpha$; on obtient

$$\delta - \delta' \equiv 0, \qquad \beta - \beta' \equiv 0.$$

Multiplions au contraire la troisième par β et la quatrième par $-\gamma$ et ajoutons; on obtient

$$\alpha - \alpha' \equiv 0, \qquad \gamma - \gamma' \equiv 0,$$

On peut procéder de la même manière en partant des hypothèses

$$\delta'\alpha - \gamma'\beta \equiv - \beta'\gamma + \alpha'\delta \equiv 1,$$
$$- \beta'\alpha + \alpha'\beta \equiv \quad \delta'\gamma - \gamma'\delta \equiv 0.$$

103. Il résulte de ce qui précède que, si l'on représente par

$$1, \quad P_1, \quad P_2, \quad \ldots$$

les substitutions de $\Gamma_{\{n\}}$, et si l'on forme pour le groupe Γ le Tableau habituel

$$(1) \qquad \left\{ \begin{array}{llll} 1 & P_1 & P_2 & \ldots, \\ Q_1 & Q_1 P_1 & Q_1 P_2 & \ldots, \\ Q_2 & Q_2 P_1 & Q_2 P_2 & \ldots, \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots, \end{array} \right.$$

les substitutions de la première ligne et celles-là seulement sont congrues à 1. Deux substitutions d'une même ligne sont congrues entre elles, tandis que celles de deux lignes différentes ne sont pas congrues. En effet :

a. Par définition, $\Gamma_{\{n\}}$ est l'ensemble des substitutions de Γ congrues à 1 ;

b. Si $P_i \equiv 1$, on a

$$Q_h P_i = Q_h,$$

d'où

$$Q_h P_i \equiv Q_h P_j ;$$

c. Si l'on avait pour $h \neq k$

$$Q_h P_l \equiv Q_k P_j,$$

on aurait aussi

$$Q_h \equiv Q_k P_j P_l^{-1} \equiv Q_k$$

et, par suite,

$$Q_h^{-1} Q_k \equiv 1.$$

Alors $Q_h^{-1} Q_k$ appartiendrait à la première ligne et, par suite, $Q_h Q_h^{-1} Q_k = Q_k$ appartiendrait à la ligne qui contient Q_h, tandis qu'elle appartient à une autre ligne.

De là résulte que le groupe $G_{\{n\}}$ est celui qu'on déduirait de Γ en considérant comme identiques les substitutions congrues suivant le module n.

Donc, pour former le groupe $G_{\{n\}}$, il suffit de prendre un système

de substitutions de Γ non congrues suivant le module n. La détermination d'un tel système nous fera connaître l'ordre de $G_{\{n\}}$, c'est-à-dire l'indice de $\Gamma_{\{n\}}$.

104. Une propriété importante des groupes $G_{\{n\}}$ est la suivante : soient S et T les substitutions de $G_{\{n\}}$ correspondant par isomorphie aux substitutions de Γ désignées par les mêmes lettres, en sorte que

$$(1) \qquad S^n = 1, \qquad T^2 = 1, \qquad (TS)^3 = 1;$$

on peut démontrer que les relations (1) sont les seules qui puissent exister entre S et T.

Supposons en effet qu'entre S et T existe une relation que, pour fixer les idées, nous écrirons sous la forme

$$(2) \qquad S^\alpha T S^\beta T S^\gamma T S^\delta = 1.$$

Sur la surface fermée correspondant au sous-groupe $\Gamma_{\{n\}}$ prenons un point intérieur au triangle 1 et traçons à partir de ce point une ligne traversant successivement les triangles

$$S,\ S^2,\ \ldots,\ S^\delta,\ TS^\delta,\ STS^\delta,\ S^2TS^\delta,\ \ldots,\ S^\gamma TS^\delta,\ \ldots,$$
$$S^\alpha TS^\beta TS^\gamma TS^\delta.$$

D'après (2), le dernier triangle se confond avec le triangle 1; nous pourrons donc revenir à notre point de départ après avoir décrit une ligne fermée. Cette ligne pourra être ramenée par une déformation continue à un ensemble de plusieurs lignes L entourant chacune un nœud du réseau. Imaginons que chacune de ces lignes soit composée de trois parties : d'abord une ligne l allant d'un point intérieur au triangle 1 à un point très voisin d'un des nœuds, ensuite un petit cercle c entourant ce nœud et enfin la ligne l considérée en premier lieu, mais parcourue en sens inverse. Or un nœud, suivant qu'il est de première, deuxième ou troisième espèce, est le transformé du pôle de la substitution T, TS ou S. Donc, M désignant un produit formé à l'aide de S et T, le circuit autour d'un nœud sera représenté par l'une des trois substitutions

$$M^{-1}T^2M, \quad M^{-1}(TS)^3M, \quad M^{-1}S^nM.$$

La ligne l considérée correspond à un certain produit composé

avec S, T, et par suite l'une quelconque des lignes fermées L sera représentée par le produit

(3) $$NM^{-1}UMN^{-1},$$

U désignant T_2, $(TS)^3$ ou S^n.

Dans tous les cas le produit (3) se réduit à l'identité en vertu des relations (1), et, par conséquent, le premier membre de (2), qui est équivalent à un produit d'expressions analogues à la précédente, se réduit identiquement à 1.

Donc la relation (2) est une conséquence des relations (1).

On déduit de là le théorème suivant, dû à WALTER DYCK :

Si S *et* T *sont deux opérations susceptibles d'engendrer un groupe et satisfaisant aux relations*

$$S^n = 1, \quad T^2 = 1, \quad (TS)^3 = 1,$$

ce groupe est holoédriquement isomorphe au groupe $G_{\{n\}}$.

105. Nous appellerons substitution *réduite* toute substitution, unitaire ou non, dont les éléments sont des nombres entiers non négatifs, inférieurs à n; et substitutions *complémentaires* deux substitutions réduites dont deux éléments homologues quelconques ont pour somme 0 ou n.

Une substitution réduite, dont le déterminant est congru à 1 *suivant le module* n, *n'est égale à sa complémentaire que pour* $n = 2$.

Soit $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une telle substitution; les nombres 2α, 2β, 2γ, 2δ, dont deux au moins ne sont pas nuls, ont pour valeur 0 ou n. Donc n doit être pair. Posons $n = 2m$: les quatre nombres α, β, γ, δ ne seront pas tous égaux à m, car autrement on aurait $\alpha\delta - \beta\gamma = 0$; deux ou trois d'entre eux seront égaux à m et les autres (ou l'autre) à 0, et l'on aura

$$\alpha\delta - \beta\gamma = \pm m^2,$$

d'où

$$\pm m^2 \equiv 1 \pmod{2m},$$

ce qui n'est possible que si $m = 1$, et par suite $n = 2$.

Deux substitutions réduites distinctes ne sont congruentes entre elles que si elles sont complémentaires.

En effet, soient les deux substitutions réduites distinctes

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix};$$

on ne peut avoir

$$\alpha' \equiv \alpha, \qquad \beta' \equiv \beta, \qquad \gamma' \equiv \gamma, \qquad \delta' \equiv \delta;$$

et pour qu'on ait

$$\alpha' \equiv -\alpha, \qquad \beta' \equiv -\beta, \qquad \gamma' \equiv -\gamma, \qquad \delta' \equiv -\delta,$$

il faut et il suffit qu'elles soient complémentaires.

Étant donnée une substitution quelconque de Γ, *on peut trouver une substitution réduite qui lui est congrue;* telle est, par exemple, la substitution formée par les *résidus minima* non négatifs de ses éléments. Il suit de là, et en vertu de ce qui a été dit plus haut, que *toute substitution modulaire est congrue à deux substitutions réduites complémentaires et à celles-là seulement;* et que *toutes les substitutions d'une même ligne du Tableau* (1) (n° 103) *sont congrues à deux substitutions réduites complémentaires et à celles-là seulement.*

Ainsi, par exemple, les éléments de la première ligne sont congrus aux deux substitutions

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} n-1 & 0 \\ 0 & n-1 \end{pmatrix}.$$

Il est évident que, si une substitution réduite $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est congrue à une substitution de Γ, ses éléments satisfont à la congruence

$$(1) \qquad \alpha\delta - \beta\gamma \equiv 1 \pmod{n}.$$

Réciproquement, *si une substitution réduite* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *satisfait à la congruence* (1), *il existe des substitutions de* Γ *qui lui sont congrues.*

Soit λ le plus grand diviseur de α qui soit premier avec n; on pourra déterminer un nombre p tel que

$$(2) \qquad np \equiv 1 - \beta \pmod{\lambda}.$$

Posons

$$(3) \qquad b = \beta + np;$$

on aura, d'après (2),

$$b \equiv 1 \pmod{\lambda}.$$

Il en résulte que b et λ sont premiers entre eux, et que α et b ne peuvent avoir aucun diviseur commun qui soit premier avec n. D'autre part, d'après (1), α, β, n et par suite aussi α, b, n sont premiers entre eux. Donc α et b ne peuvent avoir aucun diviseur commun qui soit en même temps un diviseur de n.

Il suit de là que l'équation indéterminée

$$(4) \qquad \alpha k - bh = q,$$

où h et k sont les deux inconnues, est résoluble quel que soit q. Or de (1) et (3) on déduit

$$\alpha\delta - b\gamma \equiv 1 \pmod{n},$$

qu'on peut écrire

$$\alpha\delta - b\gamma \equiv 1 + nq$$

ou, en combinant cette relation avec (4),

$$\alpha(\delta - nk) - b(\gamma - nh) = 1,$$

en sorte que la substitution

$$\begin{pmatrix} \alpha & \beta + np \\ \gamma - nh & \delta - nk \end{pmatrix}$$

appartient à Γ. D'autre part, elle est congrue à la substitution réduite donnée. Notre proposition est donc établie.

Ce résultat montre qu'étant donnée une substitution réduite satisfaisant à (1), il existe une ligne de Tableau (1) (n° 103) formée par les substitutions qui lui sont congrues.

Nous pouvons donc prendre comme éléments du groupe $G_{\{n\}}$ des substitutions réduites satisfaisant à (1) moyennant les conventions suivantes :

De deux substitutions complémentaires on en prendra une et une seule ;

Au lieu du produit de deux substitutions réduites, on devra considérer la substitution réduite congrue à ce produit.

106. Désignons par $\mu(n)$ l'ordre de $G_{\{n\}}$, c'est-à-dire l'indice

de $\Gamma_{(n)}$; on peut représenter ces derniers groupes respectivement par $G_{\mu(n)}$, $\Gamma_{\mu(n)}$. Le nombre $\mu(n)$ est la moitié du nombre de substitutions réduites dont le déterminant est congru à 1, sauf dans le cas de $n = 2$ où $\mu(n)$ est précisément égal au nombre de ces substitutions.

Si l'on considère des substitutions homogènes, par rapport à deux variables, au lieu de $G_{\mu(n)}$ on a un groupe $G_{2\mu(n)}$ d'ordre $2\mu(n)$: dans ce cas, en effet, deux substitutions ne doivent être regardées comme congrues que si

$$\alpha' \equiv \alpha, \qquad \beta' \equiv \beta, \qquad \gamma' \equiv \gamma, \qquad \delta' \equiv \delta,$$

et non pas si

$$\alpha' \equiv -\alpha, \qquad \beta' \equiv -\beta, \qquad \gamma' \equiv -\gamma, \qquad \delta' \equiv -\delta.$$

Cherchons à déterminer $2\mu(n)$, c'est-à-dire le nombre des solutions non congrues de

(1) $$\alpha\delta - \beta\gamma \equiv 1 \qquad (\text{mod}\, n).$$

Faisons d'abord une remarque.

Soit $n = n_1 n_2$, n_1 et n_2 étant premiers entre eux.

Chaque solution de (1) constitue une solution de chacune des deux congruences

(2) $$\alpha\delta - \beta\gamma \equiv 1 \qquad (\text{mod}\, n_1), \qquad \alpha\delta - \beta\gamma \equiv 1 \qquad (\text{mod}\, n_2).$$

Réciproquement, tout couple de solutions α_1, β_1, γ_1, δ_1; α_2, β_2, γ_2, δ_2 des congruences (2) donne lieu à une solution α, β, γ, δ de (1). En effet, puisque n_1 et n_2 sont premiers entre eux, chacune des congruences

$$n_1 a + \alpha_1 \equiv \alpha_2, \qquad n_1 b + \beta_1 \equiv \beta_2, \qquad n_1 c + \gamma_1 \equiv \gamma_2, \qquad n_1 d + \delta_1 \equiv \delta_2 \qquad (\text{mod}\, n_2),$$

où les inconnues sont a, b, c, d, admet une solution et une seule.

Une fois trouvées a, b, c, d, les nombres

$$\alpha = n_1 a + \alpha_1,$$
$$\beta = n_1 b + \beta_1,$$
$$\gamma = n_1 c + \gamma_1,$$
$$\delta = n_1 d + \delta_1$$

satisfont à (1).

Il suit de là que

$$(3) \qquad 2\mu(n_1 n_2) = 2\mu(n_1)\, 2\mu(n_2).$$

Il suffira donc de déterminer l'expression de $\mu(n)$ dans le cas où n est une puissance d'un nombre premier.

Soit $n = p^r$, p étant un nombre premier.

Si α n'est pas divisible par p et $0 \leqq \beta < p^r$, la congruence

$$(4) \qquad \alpha\delta - \beta\gamma \equiv 1 \quad (\bmod p^r)$$

donne pour chaque valeur arbitraire de γ une valeur de δ et une seule, non négative et inférieure à p^r. Puisque le nombre des valeurs possibles incongrues de γ est p^r, à deux valeurs données de α, β correspondent p^r couples de valeurs γ, δ.

Si α est divisible par p, β ne l'est pas, et alors, pour chaque valeur de δ prise arbitrairement, on a une seule valeur de γ et, dans ce cas encore, p^r couples de valeurs γ, δ.

Donc à chaque couple de valeurs α, β moindres que p^r et non divisibles toutes deux par p, correspondent p^r couples de valeurs γ, δ satisfaisant à la congruence (4).

Calculons le nombre des couples de $\alpha\beta$. Les valeurs de α moindres que p^r et non divisibles par p, en nombre $p^r - p^{r-1}$, peuvent être associées à chaque valeur de β moindre que p^r, ce qui donne lieu à $p^r(p^r - p^{r-1})$ couples; au contraire, les valeurs de α divisibles par p, en nombre p^{r-1}, peuvent être associées aux valeurs de β non divisibles par p, d'où $p^{r-1}(p^r - p^{r-1})$ couples.

Le nombre total des couples est donc

$$(p^r + p^{r-1})(p^r - p^{r-1}) = p^{2r}\left(1 - \frac{1}{p^2}\right),$$

ce qui donne

$$p^{3r}\left(1 - \frac{1}{p^2}\right)$$

solutions de (4) et, par suite,

$$(5) \qquad 2\mu(p^r) = p^{3r}\left(1 - \frac{1}{p^2}\right).$$

Si donc

$$n = p_1^{r_1} p_2^{r_2} \ldots p_h^{r_h},$$

la relation (3) montre que

$$2\mu(n) = n^3\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\cdots\left(1-\frac{1}{p_h^2}\right).$$

Pour le cas de $p=2$, $r=1$, il faut remplacer dans la formule (5) $2\mu(p^r)$ par $\mu(p^x)$.

La relation (5) donne

$$\mu(2)=6,\qquad \mu(3)=12,\qquad \mu(4)=24,\qquad \mu(5)=60,$$

en sorte que les groupes $\Gamma_{\mu(n)}$ et $\Gamma_{[n]}$ coïncident pour $n=2, 3, 4, 5$. Mais cette coïncidence cesse dès que $n>5$; en effet $\Gamma_{\mu(n)}$ est un sous-groupe de Γ d'indice fini, tandis que (n° 98) $\Gamma_{[n]}$ est un sous-groupe d'indice infini.

107. Supposons que n puisse être décomposé en deux facteurs n_1, n_2 premiers entre eux

$$n = n_1 n_2;$$

alors

$$2\mu(n) = 2\mu(n_1)\,2\mu(n_2).$$

Si P et Q désignent deux substitutions homogènes quelconques, le groupe $G_{2\mu(n)}$ du paragraphe précédent contient une substitution S et une seule, telle que

$$S \equiv P \pmod{n_1},\qquad S\equiv Q \pmod{n_2}.$$

Remplaçons P successivement par toutes les substitutions du groupe $G_{2\mu(n_1)}$, et faisons $Q\equiv 1$; nous obtiendrons pour S un système de $2\mu(n_1)$ substitutions homogènes incongrues suivant n_1 et toutes congrues à 1 suivant n_2.

Ce système est manifestement un groupe, il ne diffère pas essentiellement du groupe $G_{2\mu(n_1)}$ et par suite peut être représenté par le même symbole. Donc $G_{2\mu(n)}$ contient $G_{2\mu(n_1)}$ comme sous-groupe.

Il est facile de voir que c'est un sous-groupe invariant : en effet, soient S une quelconque de ses substitutions et T une substitution quelconque du groupe $G_{2\mu(n)}$, on a

$$T^{-1}ST \equiv T^{-1}T \equiv 1 \pmod{n_2}.$$

De même $G_{2\mu(n)}$ contient $G_{2\mu(n_2)}$ comme sous-groupe invariant. De plus, les substitutions des deux sous-groupes sont permutables. En effet, soient S_1 et S_2 deux substitutions quelconques de $G_{2\mu(n_1)}$ et $G_{2\mu(n_2)}$, en sorte que

$$S_1 \equiv 1 \pmod{n_2}, \qquad S_2 \equiv 1 \pmod{n_1};$$

on a alors

$$S_1 S_2 \equiv \begin{cases} S_1 & \pmod{n_1} \\ S_2 & \pmod{n_2} \end{cases}, \qquad S_2 S_1 \equiv \begin{cases} S_1 & \pmod{n_1} \\ S_2 & \pmod{n_2} \end{cases},$$

d'où

$$S_1 S_2 \equiv S_2 S_1.$$

On peut donc appliquer au groupe $G_{2\mu(n)}$ les considérations du n° **14**, permettant de construire les sous-groupes de $G_{2\mu(n)}$ quand on connaît ceux de $G_{2\mu(n_1)}$ et $G_{2\mu(n_2)}$. On peut donc, dans la recherche directe des sous-groupes de $G_{2\mu(n)}$, se borner au cas où n est une puissance d'un nombre premier.

Nous examinerons seulement le cas extrêmement simple où n est un nombre premier.

108. Mais, auparavant, il convient de donner quelques explications sur certains symboles introduits par Galois dans la théorie des nombres.

Si N n'est pas un résidu quadratique d'un nombre premier, la congruence

$$x^2 \equiv N \pmod{p}$$

n'a pas de solutions.

Introduisons, comme dans la théorie des imaginaires, un symbole ε défini par la congruence

$$\varepsilon^2 \equiv N \pmod{p}.$$

Nous appellerons ε un *nombre imaginaire* et nous désignerons sous le nom de *nombres complexes* les expressions de la forme $a + b\varepsilon$, a et b étant des entiers ordinaires.

Deux nombres complexes $a + b\varepsilon$ et $a' + b'\varepsilon$ sont dits *égaux* si $a = a'$, $b = b'$. En particulier, un nombre complexe $a + b\varepsilon$ est nul si $a = 0$, $b = 0$.

Les nombres $a+b\varepsilon$, $a-b\varepsilon$ sont dits *conjugués;* soit $a+b\varepsilon=\mathbf{a}$, nous écrirons $a-b\varepsilon=\bar{\mathbf{a}}$.

Deux nombres conjugués ne peuvent être égaux que s'ils sont réels.

Si l'on a

$$\mathbf{a}\bar{\mathbf{a}}\equiv 0,$$

il en résulte

$$\mathbf{a}\equiv\bar{\mathbf{a}}\equiv 0.$$

En effet, on peut écrire

$$0\equiv\mathbf{a}\bar{\mathbf{a}}\equiv a^2-b^2\mathrm{N}$$

ou bien

$$a^2\equiv b^2\mathrm{N}.$$

Mais si a^2 et b^2 ne sont pas nuls, a^2 est un résidu quadratique, tandis que b^2 est un non-résidu, donc la congruence ne peut avoir lieu que si $a\equiv b\equiv 0$, c'est-à-dire

$$\mathbf{a}\equiv\bar{\mathbf{a}}\equiv 0.$$

Si $\mathbf{a}$, $\mathbf{b}$ *sont deux nombres complexes* et si $\mathbf{ab}\equiv 0$, *on doit avoir soit* $\mathbf{a}\equiv 0$, *soit* $\mathbf{b}\equiv 0$.

Supposons

$$\mathbf{a}=a+b\varepsilon\not\equiv 0,\qquad \mathbf{b}=a'+b'\varepsilon.$$

De l'hypothèse faite il résulte

$$0\equiv\bar{\mathbf{a}}\mathbf{ab}=(a^2-b^2\mathrm{N})(a'+b'\varepsilon)=(a^2-b^2\mathrm{N})a'+(a^2-b^2\mathrm{N})b'\varepsilon,$$

d'où

$$(a^2-b^2\mathrm{N})a'\equiv(a^2-b^2\mathrm{N})b'=0;$$

mais

$$a^2-b^2\mathrm{N}\not\equiv 0,$$

donc $a'\equiv b'\equiv 0$ et, par suite, $\mathbf{b}\equiv 0$.

Dans le champ des nombres ordinaires et complexes *toute congruence du second degré* (suivant un module premier) *a deux racines* (*et deux seulement*), égales ou distinctes.

En effet, la congruence

$$(1)\qquad ax^2+2bx+c=0\qquad (\mathrm{mod}\,p)$$

peut s'écrire

$$(2)\qquad (ax+b)^2 \equiv b^2 - ac \pmod{p}.$$

Si $b^2 - ac$ est un résidu de p, il existe comme on sait deux racines de (2) et par suite de (1); si $b^2 - ac$ est un non-résidu, on pourra poser, d étant un certain nombre,

$$b^2 - ac \equiv d^2 \mathrm{N} \pmod{p},$$

d'où

$$ax + b \equiv \pm d\varepsilon \pmod{p},$$
$$x \equiv -be \pm de\varepsilon \pmod{p},$$

e représentant le nombre qui satisfait à la congruence

$$ae \equiv 1 \pmod{p}.$$

On démontre, comme pour des nombres ordinaires, qu'*une congruence de degré m suivant un module premier ne peut avoir plus de m racines.*

Soient

$$\mathbf{a} = a + b\varepsilon, \qquad \bar{\mathbf{a}} = a - b\varepsilon$$

deux nombres complexes conjugués. On aura

$$\mathbf{a}^p = a^p + \binom{p}{1} a^{p-1} b\varepsilon + \binom{p}{2} a^{p-2} b^2 \varepsilon^2 + \ldots + b^p \varepsilon^p$$
$$\equiv a^p + b^p \varepsilon^p \equiv a + b\varepsilon \mathrm{N}^{\frac{p-1}{2}},$$

puisque, d'après le théorème de FERMAT, $a^{p-1} \equiv b^{p-1} \equiv 1$.

De plus, N étant un non-résidu de p, $\mathrm{N}^{\frac{p-1}{2}} \equiv -1$, et alors

$$\mathbf{a}^p \equiv a - b\varepsilon = \bar{\mathbf{a}}.$$

De même

$$\bar{\mathbf{a}}^p \equiv \mathbf{a}, \qquad \text{d'où} \qquad \mathbf{a}^{p^2} \equiv \mathbf{a},$$

et, par conséquent,

$$(3)\qquad \mathbf{a}^{p^2-1} \equiv 1.$$

Cette dernière formule est la *généralisation du théorème de* FERMAT.

Il suit de là que la congruence

$$(4)\qquad x^{p^2-1} \equiv 1 \pmod{p}$$

a précisément un nombre de racines égal à son degré; en effet elle est satisfaite par tous les nombres complexes $a + b\varepsilon$ non congrus à zéro suivant le module p, et leur nombre est précisément $p^2 - 1$, a et b pouvant prendre n'importe quel couple de valeurs sauf le couple 0,0.

De ce théorème on déduit la conséquence suivante : *Si q est un diviseur de $p^2 - 1$, la congruence*

$$x^q \equiv 1 \pmod{p}$$

a q racines.

La démonstration est la même que pour les nombres ordinaires.

Il peut arriver qu'une racine $\mathbf{a}$ de la congruence (4) soit aussi racine d'une autre congruence de la forme

$$x^r \equiv 1 \pmod{p}$$

où $r < p^2 - 1$. On démontre facilement que si r est le plus petit nombre pour lequel $\mathbf{a}^r \equiv 1$, $p^2 - 1$ est un multiple de r. On dit que le nombre $\mathbf{a}$ *appartient* à l'exposant r; les nombres appartenant à l'exposant $p^2 - 1$ s'appellent *racines primitives* de p.

Si les nombres $\mathbf{a}_1$, $\mathbf{a}_2$ appartiennent respectivement aux exposants r_1, r_2 premiers entre eux, le nombre [1] $\mathbf{a} = \mathbf{a}_1 \mathbf{a}_2^{-1}$ *appartient à l'exposant $r = r_1 r_2$.*

Soit, pour un certain nombre s, $\mathbf{a}^s \equiv 1$, d'où $\mathbf{a}_1^s \equiv \mathbf{a}_2^s$. Posons

$$\mathbf{a}_1^s \equiv \mathbf{a}_2^s \equiv \mathbf{b};$$

si t_1 est le plus grand commun diviseur de r_1 et de s, t_2 celui de

---

(1) La notation a^{-1} indique, dans la théorie des nombres, le nombre b satisfaisant à la congruence

$$ab \equiv 1 \pmod{p}.$$

Ce nombre existe toujours et est déterminé d'une manière unique relativement au module p, quand p est premier et a n'est pas multiple de p, ou plus généralement quand a est premier avec p. De même, on représente par ca^{-1} le nombre b qui satisfait à la congruence

$$ab \equiv c \pmod{p}.$$

r_2 et de s, on aura

$$\mathbf{a}_1^{s\frac{r_1}{t_1}} = \mathbf{a}_1^{r_1\frac{s}{t_1}} \equiv 1, \qquad \mathbf{a}_2^{s\frac{r_2}{t_2}} = \mathbf{a}_2^{r_2\frac{s}{t_2}} \equiv 1,$$

d'où

$$\mathbf{b}^{\frac{r_1}{t_1}} = \mathbf{b}^{\frac{r_2}{t_2}} \equiv 1.$$

Or, r_1 et r_2 sont premiers entre eux; donc il en est de même de $\frac{r_1}{t_1}$, $\frac{r_2}{t_2}$ et, par suite, d'après la relation précédente

$$\mathbf{b} \equiv 1,$$

ou bien

$$\mathbf{a}_1^s \equiv \mathbf{a}_2^s \equiv 1.$$

Il résulte de là que s doit être un multiple commun à r_1 et à r_2. Donc la plus petite valeur de s pour laquelle $\mathbf{a}^s \equiv 1$ est $s = r_1 r_2$.

Tout nombre premier p admet des racines primitives et plus généralement *il existe des nombres appartenant à tout exposant, qui est un diviseur de $p^2 - 1$.*

Soit

$$p^2 - 1 = p_1^{r_1} p_2^{r_2} \ldots$$

où p_1, p_2 représentent des facteurs premiers différents.

Si q est un diviseur de $p^2 - 1$, on aura

$$q = p_1^{s_1} p_2^{s_2} \ldots$$

avec

$$s_1 \leqq r_1, \qquad s_2 \leqq r_2, \qquad \ldots.$$

Puisque $p_1^{s_1}$ est un diviseur de $p^2 - 1$, la congruence $x^{p_1^{s_1}} \equiv 1$ a $p_1^{s_1}$ racines; certaines d'entre elles sont d'exposant $p_1^{s_1}$, sans quoi elles seraient toutes racines de la congruence

$$x^{p_1^{s_1 - 1}} \equiv 1.$$

Il existe donc des nombres appartenant à l'exposant $p_1^{s_1}$ et aussi des nombres appartenant à l'exposant $p_2^{s_2}$, etc. Au moyen de ces nombres, et en vertu du théorème précédent, on peut former des nombres appartenant à l'exposant q.

Soient en particulier

$$q = p + 1$$

et $\mathbf{t}$ un nombre appartenant à l'exposant q; les racines de la congruence

$$(5) \qquad x^{p+1} \equiv 1$$

seront

$$(6) \qquad 1, \quad \mathbf{t}, \quad \mathbf{t}^2, \quad \ldots, \quad \mathbf{t}^{p-1}, \quad \mathbf{t}^p \equiv \mathbf{t}^{-1}.$$

De la relation générale $\mathbf{a}^p \equiv \overline{\mathbf{a}}$ trouvée précédemment on déduit

$$\mathbf{t}^p \equiv \mathbf{t}^{-1} \equiv \overline{\mathbf{t}}.$$

D'autre part, on ne peut avoir $\mathbf{t}^p \equiv \mathbf{t}$, car il en résulterait

$$\mathbf{t}^{p-1} \equiv 1,$$

et $\mathbf{t}$ n'appartiendrait pas à l'exposant $p+1$. D'où il suit que $\mathbf{t}$ *n'est pas réel.*

Posons donc

$$\mathbf{t} = c + d\varepsilon,$$

d n'est ni nul, ni multiple de p.

D'après cela, étant donné un nombre complexe quelconque

$$\mathbf{a} = a + b\varepsilon,$$

on peut trouver un nombre ordinaire l tel qu'on ait

$$ld \equiv b \qquad (\bmod p),$$

d'où

$$\mathbf{a} \equiv a + l\,d\varepsilon = (a - lc) + l\mathbf{t} \qquad (\bmod p),$$

en sorte que tout nombre complexe peut être mis sous la forme $h + k\mathbf{t}$.

Si $\mathbf{a}\overline{\mathbf{a}} \equiv 1$, $\mathbf{a}$ est *une puissance de* $\mathbf{t}$.

En effet, comme $\overline{\mathbf{a}} \equiv \mathbf{a}^p$, on a dans le cas actuel $\mathbf{a}^{p+1} \equiv 1$, en sorte que $\mathbf{a}$ est une racine de la congruence (5) et par suite est une des quantités (6).

Les substitutions linéaires

$$(7) \qquad \xi' = \frac{\mathbf{a}\xi + \mathbf{b}}{\overline{\mathbf{b}}\xi + \overline{\mathbf{a}}}$$

où $\mathbf{a}$ *et* $\mathbf{b}$ *sont deux nombres complexes liés par la relation*

$$\mathbf{a}\bar{\mathbf{a}} - \mathbf{b}\bar{\mathbf{b}} \equiv 1 \pmod p$$

forment un groupe.

En effet, si

$$\xi' = \frac{\mathbf{a}'\xi + \mathbf{b}'}{\bar{\mathbf{b}}'\xi + \bar{\mathbf{a}}'}$$

est une autre substitution de même nature, c'est-à-dire telle que

$$\mathbf{a}'\bar{\mathbf{a}}' - \mathbf{b}'\bar{\mathbf{b}}' \equiv 1 \pmod p,$$

le produit des deux substitutions est

$$\xi' = \frac{(\mathbf{a}'\mathbf{a} + \mathbf{b}'\bar{\mathbf{b}})\xi + (\mathbf{a}'\mathbf{b} + \mathbf{b}'\bar{\mathbf{a}})}{(\bar{\mathbf{b}}'\mathbf{a} + \bar{\mathbf{a}}'\bar{\mathbf{b}})\xi + (\bar{\mathbf{b}}'\mathbf{b} + \bar{\mathbf{a}}'\bar{\mathbf{a}})},$$

et l'on a

$$(\mathbf{a}'\mathbf{a} + \mathbf{b}'\bar{\mathbf{b}})(\bar{\mathbf{b}}'\mathbf{b} + \bar{\mathbf{a}}'\bar{\mathbf{a}}) - (\mathbf{a}'\mathbf{b} + \mathbf{b}'\bar{\mathbf{a}})(\bar{\mathbf{b}}'\mathbf{a} + \bar{\mathbf{a}}'\bar{\mathbf{b}})$$
$$= (\mathbf{a}\bar{\mathbf{a}} - \mathbf{b}\bar{\mathbf{b}})(\mathbf{a}'\bar{\mathbf{a}}' - \mathbf{b}'\bar{\mathbf{b}}') \equiv 1.$$

La transformée d'une substitution quelconque $\xi' = \mathrm{P}(\xi)$ de la forme (7), *par une substitution*

$$\xi' = \mathrm{A}(\xi) = \frac{-\xi + 1}{\varepsilon\xi + \varepsilon}$$

[qui n'appartient pas au groupe (7)] *est une substitution* $\xi' = \mathrm{P}(\xi)$ *du groupe* $\mathrm{G}_{\mu(p)}$ *et la somme des éléments extrêmes est la même dans les deux substitutions.*

Posons en effet

$$\mathbf{a} = m + n\varepsilon, \qquad \mathbf{b} = r + s\varepsilon;$$

on trouve

$$\mathrm{A}^{-1}\mathrm{P}\,\mathrm{A}(\xi) = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}$$

avec

$$\alpha = m - r, \qquad \beta = -n - s, \qquad \gamma = -\mathrm{N}(n - s), \qquad \delta = m + r;$$

de plus

$$\alpha\delta - \beta\gamma \equiv 1 \pmod p, \qquad \alpha + \delta = \mathbf{a} + \bar{\mathbf{a}}.$$

Il suit de là que *le groupe des substitutions* (7) est holoédriquement *isomorphe au groupe* $\mathrm{G}_{\mu(p)}$. Donc dans les questions

purement formelles, c'est-à-dire où l'on fait abstraction de la nature des opérations qui composent les groupes, il est indifférent de considérer l'un ou l'autre de ces deux groupes.

Nous représenterons le groupe (7) par $G_{\mu(p)}$.

109. Ces notions établies, arrivons à la recherche des sous-groupes du groupe $G_{\mu(p)}$ et observons de suite que, p étant premier, on a

$$\mu(p) = \frac{p(p^2-1)}{2} \quad (^1).$$

Commençons par les sous-groupes cycliques d'ordre p.

L'un d'eux, G_p, se construit immédiatement; il est formé de l'identité, de la substitution

$$S(z) = z + 1$$

et des puissances 2e, 3e, ..., $(p-1)^{\text{ième}}$ de $S(z)$.

Pour trouver d'autres sous-groupes cycliques, considérons d'abord ceux qui sont équivalents à G_p.

Soit $P \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une substitution quelconque de $G_{\mu(p)}$.

On a (*voir* n° **91**)

$$(1) \qquad P^{-1} S^r P = \begin{pmatrix} 1 - r\alpha\gamma & r\alpha^2 \\ -r\gamma^2 & 1 + r\alpha\gamma \end{pmatrix}.$$

Pour que P soit permutable avec G_p, il faut que la substitution (1) soit une certaine puissance S^s de S et, par suite, qu'on ait $\gamma \equiv 0$. Il est facile de voir que cette condition est suffisante.

Maintenant si $\gamma \equiv 0$, on a

$$\alpha\delta \equiv 1;$$

alors α peut prendre toutes les $p-1$ valeurs incongrues suivant p, et à chacune d'elles correspond une valeur unique de δ, et β peut prendre p valeurs incongrues. Nous avons donc en tout $p(p-1)$ substitutions de $G_{\mu(p)}$, permutables avec G_p. Mais elles sont

---

(1) La formule serait inexacte pour $p = 2$ (*voir* n° 106); nous supposerons que p est un nombre premier impair.

deux à deux égales, puisque

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{pmatrix}$$

sont une seule et même substitution.

Donc, il y a $\frac{p(p-1)}{2}$ substitutions de $G_{\mu(p)}$ distinctes, permutables avec G_p. Il résulte de là (n° 13) que le nombre des sous-groupes équivalents à G_p, y compris G_p, est $\frac{p(p^2-1)}{2} : \frac{p(p-1)}{2}$ ou $p+1$. Les substitutions de ces groupes (en faisant abstraction de l'identité) sont toutes différentes. En effet, si deux d'entre eux avaient en commun plus d'une substitution, le nombre des substitutions communes, c'est-à-dire l'ordre du sous-groupe commun, devrait être un diviseur de l'ordre commun p des deux groupes, ordre que nous savons être premier. Donc le nombre total des substitutions contenues dans les $p+1$ sous-groupes équivalents est $(p+1)(p-1)$ ou p^2-1, sans compter l'identité.

Si l'on représente en général par σ la demi-somme du premier et du dernier élément d'une substitution, il résulte de (1) que, pour les substitutions des sous-groupes considérées, $\sigma = 1$. Naturellement, on peut aussi écrire $\sigma = -1$, puisqu'il est permis de changer le signe de tous les éléments d'une substitution. On peut donc dire que pour *les substitutions du sous-groupe* G_p *et des sous-groupes équivalents,* on a

$$\sigma^2 = 1.$$

110. Déterminons les sous-groupes cycliques d'ordre $\frac{p-1}{2}$.

Si a est une racine primitive de p, au sens ordinaire, la substitution du groupe $G_{\mu(p)}$

$$R = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

engendre un groupe cyclique $G_{\frac{p-1}{2}}$ d'ordre $\frac{p-1}{2}$. En effet, on a

$$R^r \equiv \begin{pmatrix} a^r & 0 \\ 0 & a^{-r} \end{pmatrix}$$

avec $a^r \not\equiv \pm 1$ pour $r < \frac{p-1}{2}$, tandis que

$$a^{\frac{p-1}{2}} \equiv (a^{-1})^{\frac{p-1}{2}} \equiv \pm 1,$$

en sorte que la première puissance de R qui soit congrue à 1 est celle d'ordre $\frac{p-1}{2}$. On trouve (n° 26)

$$(1) \qquad P^{-1}R^rP = \begin{bmatrix} \alpha\delta a^r - \beta\gamma a^{-r} & -\alpha\beta(a^r - a^{-r}) \\ \gamma\delta(a^r - a^{-r}) & \alpha\delta a^{-r} - \beta\gamma a^r \end{bmatrix}.$$

Supposons d'abord que $\alpha\beta$ et $\gamma\delta$ ne sont pas tous deux nuls; pour que cette substitution soit une puissance de R, il faut que

$$a^r - a^{-r} \equiv 0,$$

c'est-à-dire $a^{2r} \equiv 1$, ce qui est impossible pour $r < \frac{p-1}{2}$.

Donc on a nécessairement

$$\alpha\beta \equiv 0, \qquad \gamma\delta \equiv 0,$$

c'est-à-dire, soit

$$\beta \equiv \gamma \equiv 0, \qquad \alpha\delta \equiv 1,$$

soit

$$\alpha \equiv \delta \equiv 0, \qquad \beta\gamma \equiv -1.$$

Les deux substitutions correspondantes sont

$$P \equiv \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \qquad P \equiv \begin{pmatrix} 0 & \alpha \\ -\alpha^{-1} & 0 \end{pmatrix}.$$

La première est une puissance de R. En effet, puisque $1, a, a^2, \ldots, a^{p-1}$ est un système complet de résidus non congrus suivant p, il existe, quel que soit α, un exposant s tel que $a^s \equiv \alpha$.

La seconde est une substitution d'ordre 2. Il existe $\frac{p-1}{2}$ substitutions de ce genre; elles sont en nombre égal à la moitié du nombre des valeurs distinctes non congrues à zéro, que peut prendre α.

Donc $G_{\frac{p-1}{2}}$ est permutable avec ses propres substitutions et aussi avec $\frac{p-1}{2}$ substitutions d'ordre 2; c'est-à-dire en tout avec $p-1$ substitutions.

Il suit de là que le nombre des sous-groupes équivalents à $G_{\frac{p-1}{2}}$, y compris $G_{\frac{p-1}{2}}$ est $\frac{d(p^2-1)}{2} : (p-1)$ ou $\frac{p(p+1)}{2}$.

On peut démontrer que ces sous-groupes n'ont, deux à deux, d'autre opération commune que l'identité. Soient R_1, R_2 les opérations génératrices de deux des sous-groupes cycliques considérés, et soit une opération commune telle que l'on ait

$$R_1^r \equiv R_2^s,$$

on pourra écrire

$$R_1^r \equiv R_2^s = R_2^{-1} R_2^s R_2 \equiv R_2^{-1} R_1^r R_2.$$

D'après cela, R_2 serait permutable avec le premier des deux sous-groupes, sans lui appartenir et pour $p < 5$ ne serait pas d'ordre 2, ce qui est impossible ([1]).

Le nombre total des substitutions diverses des $\frac{p(p+1)}{2}$ sous-groupes est donc, outre l'identité $\frac{p(p+1)}{2} \times \frac{p-3}{2}$:

$$\frac{p(p+1)(p-3)}{4}.$$

Pour chacune de ces substitutions, on a, d'après la formule (1),

$$\sigma \equiv \frac{a^r + a^{-r}}{2},$$

d'où

$$\sigma^2 - 1 \equiv \left(\frac{a^r - a^{-r}}{2}\right)^2,$$

ce qu'on peut écrire

$$\sigma^2 - 1 = R,$$

R désignant un résidu quadratique de p.

111. Déterminons maintenant les sous-groupes cycliques d'ordre $\frac{p+1}{2}$. Le procédé est analogue à celui du paragraphe précédent, avec cette différence que a est remplacé par $\mathbf{t}$.

([1]) Pour $p = 5$ le sous-groupe $G_{\frac{p-1}{2}}$ et ses équivalents sont d'ordre 2 et par suite ne peuvent avoir d'autre substitution commune que l'identité.

La substitution du groupe $\mathbf{G}_{\mu(p)}$

$$\mathbf{R} = \begin{pmatrix} \mathbf{t} & 0 \\ 0 & \mathbf{t}^{-1} \end{pmatrix}$$

engendre un sous-groupe $\mathbf{G}_{\frac{p+1}{2}}$ d'ordre $\frac{p+1}{2}$. En effet, on a

$$\mathbf{R}^r = \begin{pmatrix} \mathbf{t}^r & 0 \\ 0 & \mathbf{t}^{-r} \end{pmatrix}$$

et $\mathbf{t}^r \not\equiv \pm 1$ pour $r < \frac{p+1}{2}$, tandis que

$$\mathbf{t}^{\frac{p+1}{2}} \equiv (\mathbf{t}^{-1})^{\frac{p+1}{2}} \equiv \pm 1.$$

En sorte que la première puissance de $\mathbf{R}$ qui soit congrue à 1 est celle d'ordre $\frac{p+1}{2}$. Si

$$\mathbf{P} = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \bar{\mathbf{b}} & \bar{\mathbf{a}} \end{pmatrix},$$

on a

(1) $$\mathbf{P}^{-1}\mathbf{R}^r\mathbf{P} \equiv \begin{bmatrix} \mathbf{a}\bar{\mathbf{a}}\mathbf{t}^r - \mathbf{b}\bar{\mathbf{b}}\mathbf{t}^{-r} & -\mathbf{a}\mathbf{b}(\mathbf{t}^r - \mathbf{t}^{-r}) \\ \bar{\mathbf{a}}\bar{\mathbf{b}}(\mathbf{t}^r - \mathbf{t}^{-r}) & \mathbf{a}\bar{\mathbf{a}}\mathbf{t}^{-r} - \mathbf{b}\bar{\mathbf{b}}\mathbf{t}^r \end{bmatrix}.$$

Pour que cette substitution soit une puissance de $\mathbf{R}^r$, il faut que l'on ait tout d'abord, en supposant que ni $\mathbf{a}$, ni $\mathbf{b}$ ne soient nuls,

$$\mathbf{t}^r - t^{-r} \equiv 0$$

ou $\mathbf{t}^{2r} \equiv 1$, ce qui est impossible pour $r < \frac{p+1}{2}$. On doit donc avoir soit $\mathbf{b} \equiv 0$, soit $\mathbf{a} \equiv 0$.

Dans le premier cas, $\mathbf{a}\bar{\mathbf{a}} \equiv 1$, donc (n° 108) $\mathbf{a}$ est une puissance de $\mathbf{t}$, soit $\mathbf{a} = \mathbf{t}^s$, d'où

$$\mathbf{P} \equiv \begin{pmatrix} \mathbf{t}^s & 0 \\ 0 & \mathbf{t}^{-s} \end{pmatrix} = \mathbf{R}^s,$$

et alors $\mathbf{P}$ appartient à $\mathbf{G}_{\frac{p+1}{2}}$.

Dans le second cas, on a

$$\mathbf{b}\bar{\mathbf{b}} \equiv -1.$$

$$\mathrm{P} \equiv \begin{pmatrix} 0 & \mathbf{b} \\ \bar{\mathbf{b}} & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & \bar{\mathbf{b}} \\ -\mathbf{b}^{-1} & 0 \end{pmatrix}$$

est alors une opération de période 2. Le nombre des opérations de ce genre est $\frac{p+1}{2}$, c'est-à-dire la moitié de celui des solutions de la congruence $\mathbf{b}\overline{\mathbf{b}} \equiv -1$, nombre qui est précisément $p+1$ (1). Donc $G_{\frac{p+1}{2}}$ est permutable avec ses propres substitutions et aussi avec $\frac{p+1}{2}$ substitutions d'ordre 2; en tout avec $p+1$ substitutions. Il en résulte que le nombre des sous-groupes équivalents à $\mathbf{G}_{\frac{p+1}{2}}$ ou à $G_{\frac{p+1}{2}}$, y compris le groupe lui-même, est

$\frac{p(p^2-1)}{2} : (p+1)$ ou $\frac{p(p-1)}{2}$.

Pour chacune de ces substitutions [*voir* formule (1)]

$$\sigma \equiv \frac{\mathbf{t}^r + \mathbf{t}^{-r}}{2},$$

d'où

$$\sigma^2 - 1 \equiv \left(\frac{\mathbf{t}^r - \mathbf{t}^{-r}}{2}\right)^2.$$

Mais $\mathbf{t}^r - \mathbf{t}^{-r}$, différence de deux nombres conjugués, est égal au produit d'un nombre ordinaire l par ε

$$\mathbf{t}^r - \mathbf{t}^{-r} = l\varepsilon,$$

par suite

$$\sigma^2 - 1 \equiv \frac{l^2}{4}\varepsilon^2 \equiv \frac{l^2}{4}\mathrm{N}$$

ou plus simplement en désignant par N le non-résidu $\frac{l^2}{4}\mathrm{N}$

$$\sigma^2 - 1 = \mathrm{N},$$

formule applicable également aux substitutions de $G_{\frac{p+1}{2}}$ et de ses

(1) Si $\mathbf{k}$ est une solution de la congruence $\mathbf{b}\overline{\mathbf{b}} \equiv -1$, toutes ses solutions sont

$$\mathbf{k}, \mathbf{kt}, \mathbf{kt}^2, \ldots, \mathbf{kt}^p.$$

En effet soit $\mathbf{k}'$ une autre solution, les congruences

$$\mathbf{k}\overline{\mathbf{k}'} \equiv -1, \quad \mathbf{k}'\overline{\mathbf{k}'} \equiv -1$$

donnent

$$(\mathbf{k}'\mathbf{k}^{-1})(\overline{\mathbf{k}'}\overline{\mathbf{k}}^{-1}) \equiv 1,$$

d'où (§ 108)

$$\mathbf{k}'\mathbf{k}^{-1} = \mathbf{t}^{\nu} \quad \text{ou} \quad \mathbf{k}' = \mathbf{kt}^{\nu},$$

équivalents, puisque (n° 108) σ a la même valeur pour les substitutions correspondantes des deux groupes $\mathbf{G}_{\mu(p)}$ et $G_{\mu(p)}$

112. Puisque pour les substitutions des groupes cycliques d'ordre p, $\sigma^2 - 1$ est congru à zéro, que c'est un résidu de p différent de zéro pour les groupes cycliques d'ordre $\frac{p-1}{2}$ et un non-résidu de p pour les groupes cycliques d'ordre $\frac{p+1}{2}$, les groupes des trois espèces ne peuvent avoir d'autre substitution commune que l'identité.

Le nombre total des substitutions qu'ils contiennent est, en y comprenant l'identité,

$$1 + (p^2 - 1) + \frac{p(p+1)(p-3)}{4} + \frac{p(p-1)^2}{4},$$

c'est-à-dire

$$\frac{p(p^2-1)}{2}.$$

Ces groupes considérés dans leur ensemble contiennent donc toutes les substitutions de $G_{\mu(p)}$, et par conséquent $G_{\mu(p)}$ ne contient comme groupes cycliques que ceux que nous avons trouvés et leurs sous-groupes.

La formation de ces sous-groupes ne présente aucune difficulté.

Tout d'abord p étant premier, G_p et les groupes équivalents ne contiennent aucun sous-groupe.

Pour $G_{\frac{p-1}{2}}$ ou un de ses équivalents, si $\mathbf{t}$ est un diviseur de $\frac{p-1}{2}$, R^t engendrera un groupe cyclique d'ordre $\frac{p-1}{2t}$, et l'on peut en dire autant de $G_{\frac{p+1}{2}}$ et de ses équivalents.

En particulier, suivant que $p \equiv \pm 1 \pmod 3$ [1], c'est-à-dire suivant que le nombre $\frac{p-1}{2}$ ou le nombre $\frac{p+1}{2}$ est divisible par 3, le sous-groupe $G_{\frac{p\mp1}{2}}$ et ses équivalents contiendront chacun un sous-groupe cyclique d'ordre 3. Le nombre des sous-groupes

---

[1] Nous laissons de côté le cas de $p = 3$, correspondant au groupe tétraédrique, dont nous avons déjà fait une étude détaillée.

cycliques d'ordre 3 de $G_{\mu(p)}$ est donc $\frac{p(p\pm 1)}{2}$ et, puisque chaque groupe cyclique d'ordre 3 contient deux substitutions d'ordre 3, le nombre des substitutions d'ordre 3 de $G_{\mu(p)}$ est $p(p\pm 1)$.

Considérons le cas du signe supérieur $(+)$. Chaque substitution de $G_{\frac{p-1}{2}}$ a la forme $\begin{pmatrix} a^r & 0 \\ 0 & a^{-r} \end{pmatrix}$; pour qu'elle soit d'ordre 3 on doit avoir

$$a^{3r} \equiv \mp 1 \pmod p$$

ou

$$a^{3r} + 1 \equiv 0 \pmod p,$$

qu'on peut écrire

$$(a^r \pm 1)(a^{2r} \mp a^r + 1) \equiv 0 \pmod p.$$

Et comme les facteurs a^r, $a^r \pm 1$ ne peuvent être congrus à zéro

$$a^r + a^{-r} \equiv \pm 1 \pmod p$$

ou

$$2\sigma \equiv \pm 1 \pmod p.$$

De même, dans l'autre cas, pour que la substitution $\begin{pmatrix} \mathbf{t}^r & 0 \\ 0 & \mathbf{t}^{-r} \end{pmatrix}$ de $\mathbf{G}_{\frac{p+1}{2}}$ soit d'ordre 3, on doit avoir

$$\mathbf{t}^{3r} \equiv \mp \pmod p,$$

d'où, comme plus haut,

$$\mathbf{t}^r + \mathbf{t}^{-r} \equiv \pm 1 \pmod p$$

ou

$$2\sigma \equiv \pm 1 \pmod p.$$

Ce résultat qui s'applique également à la substitution correspon-pante de $G_{\mu(p)}$ (*voir* n° 108, III) s'étend immédiatement à toutes les substitutions d'ordre 3 de $G_{\mu(p)}$; car on voit facilement qu'elles appartiennent à des sous-groupes équivalents (d'ordre 3) des sous-groupes équivalents $\left(\text{d'ordre } \frac{p\mp 1}{2}\right)$.

Cette relation

$$2\sigma \equiv \pm 1 \pmod p,$$

caractérise les substitutions d'ordre 3 de $G_{\mu(p)}$. En effet de

$$a^r + a^{-r} \equiv \pm 1$$

on déduit, en élevant les deux membres au cube,

$$a^{3r} + a^{-3r} + 3(a^r + a^{-r}) \equiv \pm 1$$

ou successivement

$$a^{3r} + a^{-3r} \pm 2 \equiv 0,$$

$$a^{6r} + 1 \pm 2a^{3r} \equiv 0,$$

$$a^{3r} \equiv \mp 1.$$

On peut faire un raisonnement analogue dans l'autre cas.

Ainsi, par exemple, selon que l'on a $p \equiv \pm 1 \pmod 4$, c'est-à-dire suivant que $\frac{p-1}{2}$ ou $\frac{p+1}{2}$ est pair, $G_{\frac{p\mp 1}{2}}$ contient un sous-groupe cyclique d'ordre 2.

Le nombre des sous-groupes cycliques d'ordre de $G_{\mu(p)}$ est donc $\frac{p(p\pm 1)}{2}$; c'est aussi le nombre des substitutions d'ordre 2.

Dans le cas du signe $+$, pour que la substitution $\begin{pmatrix} a^r & 0 \\ 0 & a^{-r} \end{pmatrix}$ de $G_{\frac{p-1}{2}}$ soit d'ordre 2, on doit avoir $a^{2r} \equiv -1$, et non pas $a^{2r} \equiv +1$, car on aurait en même temps $a^r \equiv a^{-r} \equiv \pm 1$, et la substitution considérée serait l'identité; ou bien on aurait encore $a^r + a^{-r} \equiv 0$, c'est-à-dire $\sigma \equiv 0$.

De même dans le cas du signe $-$.

La relation $a^r + a^{-r} \equiv 0$ caractérise bien les substitutions d'ordre 2, puisqu'on en déduit

$$a^{2r} \equiv -1.$$

113. Passons à la construction des sous-groupes non cycliques de $G_{\mu(p)}$.

Considérons d'abord le groupe maximum admettant comme sous-groupe invariant le sous-groupe G_p déjà étudié (n° 109). Comme on l'a vu, il est d'ordre $\frac{p(p-1)}{2}$ et comprend les substitutions de la forme $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$, où β est arbitraire et α soumis à la seule condition de ne pas être congru à zéro. Prenons la substitution pour laquelle $\beta \equiv 0$, et où α est une racine primitive de p, elle engendre un groupe cyclique $G_{\frac{p-1}{2}}$ (n° 110).

Le groupe $G_{\frac{p(p-1)}{2}}$ contient, outre $G_{\frac{p-1}{2}}$, les groupes équivalents $S^{-r}G_{\frac{p-1}{2}}S^r$, qui diffèrent tous entre eux, puisque, comme il est facile de le vérifier, $G_{\frac{p-1}{2}}$ et S ne sont pas permutables. Le sous-groupe G_p, les p groupes cycliques précédents d'ordre $\frac{p-1}{2}$ et leurs sous-groupes sont les seuls sous-groupes cycliques de $G_{\frac{p(p-1)}{2}}$. Car le nombre des substitutions distinctes comprises dans ces groupes est

$$1+(p-1)+p\left(\frac{p-1}{2}-1\right)=\frac{p(p-1)}{2}.$$

C'est précisément le nombre total des substitutions de $G_{\frac{p(p-1)}{2}}$.

Le sous-groupe $G_{\frac{p(p-1)}{2}}$, par sa définition même, n'étant pas permutable avec ses propres substitutions, appartient à un système de

$$\frac{p(p^2-1)}{2}:\frac{p(p-1)}{2}=p+1$$

sous-groupes équivalents à $G_{\mu(p)}$. On dit que ces sous-groupes sont *hémimétacycliques*.

Si t est un diviseur de $\frac{p-1}{2}$, le sous-groupe cyclique $G_{\frac{p-1}{2t}}$ (n° **112**) nous permettra d'obtenir, comme plus haut, un sous-groupe non cyclique $G_{\frac{p(p-1)}{2t}}$ de $G_{\mu(p)}$.

Les sous-groupes ainsi construits sont les seuls renfermant un sous-groupe cyclique d'ordre p. Pour le démontrer, il suffit de faire voir que les seuls sous-groupes de $G_{\mu(p)}$ contenant G_p sont $G_{\frac{p(p-1)}{2}}$ et quelques-uns de ses sous-groupes. Soit en effet G_q, un sous-groupe de $G_{\mu(p)}$ différent de $G_{\frac{p(p-1)}{2}}$, contenant G_p, mais non contenu dans $G_{\frac{p(p-1)}{2}}$.

Le groupe G_q contiendra au moins une substitution

$$Q\equiv\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix},$$

dans laquelle $\gamma\not\equiv 0$ et comme S appartient à G_p et par suite à G_q,

on voit que les trois substitutions

$$S^{(1-\delta)\gamma^{-1}} Q S^{(1-\alpha)\gamma^{-1}} = Q_1 \equiv \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix},$$

$$Q_1^{\gamma^{-1}} \equiv \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

$$S Q_1^{\gamma^{-1}} S \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = T$$

appartiennent aussi à G_q. Donc G_q contenant S et T, doit coïncider avec $G_{\mu(p)}$.

114. Considérons maintenant le groupe des substitutions de $G_{\mu(p)}$ permutables avec $G_{\frac{p-1}{2}}$. Il comprend les substitutions de $G_{\frac{p-1}{2}}$ et $\frac{p-1}{2}$ autres *substitutions* d'ordre 2; ces $p-1$ substitutions forment un groupe diédrique. Il existe $\frac{p(p+1)}{2}$ groupes de ce genre, tous équivalents.

En partant de $G_{\frac{p+1}{2}}$, on trouve de même $\frac{p(p-1)}{2}$ groupes diédriques équivalents d'ordre $p+1$.

La recherche des sous-groupes contenus dans ces groupes diédriques ne présente aucune difficulté.

Occupons-nous seulement de ceux d'entre eux qui sont trirectangles.

Soit d'abord $p \equiv 1 \pmod 4$. Alors, le groupe diédrique G_{p-1} contient l'opération $R^{\frac{p-1}{4}}$ qui est d'ordre 2. De plus, le polygone auquel se réduit le polyèdre, ayant un nombre pair $\frac{p-1}{2}$ de côtés, ses axes de symétrie sont deux à deux orthogonaux, de sorte qu'il y a $\frac{p-1}{4}$ couples d'axes de symétrie orthogonaux (axes équatoriaux) formant chacun un trièdre trirectangle avec l'axe de rotation R (axe polaire). Les deux rotations d'angle π, dont les axes sont orthogonaux et la rotation $R^{\frac{p-1}{4}}$ forment donc, avec l'identité, un groupe trirectangle. On obtient ainsi $\frac{p-1}{4}$ groupes.

Tous ces groupes sont équivalents si $\frac{p-1}{4}$ est impair, parce que les couples d'axes précédents se composent chacun d'une médiane et d'une diagonale du polygone; tandis que, si $\frac{p-1}{4}$ est pair, une moitié de ces couples comprend deux médianes, et l'autre moitié deux diagonales, en sorte que les groupes trirectangles comprennent deux systèmes de $\frac{p-1}{8}$ groupes équivalents.

Le sous-groupe G_{p-1} appartient à un système de $\frac{p(p+1)}{2}$ sous-groupes équivalents, puisqu'il y a en tout $\frac{p-1}{4}\frac{p(p+1)}{2}$ sous-groupes trirectangles. Mais il est évident que chacune de ces figures est répétée trois fois, puisque chacun des axes peut être considéré comme un axe polaire successivement dans les trois rotations.

Il y a donc $\frac{p(p^2-1)}{24}$ sous-groupes trirectangles de $G_{p(p)}$: ils sont tous équivalents ou se partagent en deux systèmes de sous-groupes équivalents suivant que $p \equiv 5$ ou $p \equiv 1 \pmod 8$.

Soit, au contraire, $p \equiv -1 \pmod 4$. Par un raisonnement analogue, on trouve que le nombre des sous-groupes trirectangles est $\frac{1}{3}\frac{p+1}{4}\frac{p(p-1)}{2}$ ou encore $\frac{p(p^2-1)}{24}$ et qu'ils forment un ou deux systèmes de sous-groupes équivalents, suivant que $p \equiv 3$ ou $p \equiv 7 \pmod 8$)

En résumé, dans tous les cas, il y a $\frac{p(p^2-1)}{24}$ sous-groupes trirectangles formant un ou deux systèmes de sous-groupes selon que

$$p \equiv \pm 3 \quad \text{ou} \quad p \equiv \pm 4 \quad (\text{mod } 8).$$

On pourrait supposer que, dans le cas

$$p \equiv \pm 1 \quad (\text{mod } 8),$$

les sous-groupes trirectangles de G_{p-1} ou de G_{p+1}, bien que n'étant pas équivalents entre eux, soient cependant équivalents, lorsqu'on les considère comme sous-groupes de $G_{\mu(p)}$; il n'en est rien. En effet, supposons que les $\frac{p(p^2-1)}{24}$ sous-groupes trirectangles soient tous équivalents, alors chacun d'eux (n° 13) est permutable avec

$$\frac{p(p^2-1)}{2} : \frac{p(p^2-1)}{24} = 12 \text{ substitutions}$$

formant un certain groupe G_{12}, dont le groupe trirectangle considéré G_4 est un sous-groupe invariant. Supposons que G_4 soit un des groupes trirectangles contenus dans le groupe cyclique $G_{p\pm 1}$. Les substitutions de G_4 seront

$$1, \quad R^{\frac{p\mp 1}{4}}, \quad P, \quad PR^{\frac{p\mp 1}{4}},$$

P étant une certaine substitution d'ordre 2. Mais si

$$p \equiv \pm 1 \pmod 8,$$

en posant

$$R^{\frac{p\mp 1}{8}} = Y,$$

le groupe diédrique d'ordre 8

$$1, \quad Y, \quad Y^2, \quad Y^3, \quad P, \quad PY, \quad PY^2, \quad PY^3$$

se compose de substitutions permutables avec G_4; il devrait donc être contenu dans G_{12}, ce qui est impossible.

On a vu qu'il y a $\frac{p(p\pm 1)}{2}$ substitutions d'ordre 2 dans $G_{\mu(p)}$, et que R et, par suite, toute autre substitution de ce genre appartient à $\frac{p\mp 1}{4}$ sous-groupes trirectangles. Si l'on observe que tout groupe trirectangle contient trois substitutions d'ordre 2, le nombre total des groupes trirectangles qui en résulte

$$\frac{1}{3}\,\frac{p\mp 1}{4}\,\frac{p(p\pm 1)}{2} = \frac{p(p^2-1)}{24}$$

est égal au nombre de groupes déjà trouvé. Donc il n'existe pas d'autres sous-groupes trirectangles que ceux qui ont été considérés.

115. Nous avons dit, un peu plus haut, que, si les $\frac{p(p^2-1)}{24}$ sous-groupes trirectangles sont équivalents entre eux, ce qui a lieu pour

$$p \equiv \pm 3 \pmod 8,$$

l'un de ces sous-groupes G_4 est permutable avec douze substitutions. Le groupe G_{12} formé par ces substitutions admet G_4 comme sous-groupe invariant. Soient $1, X_1, X_2, X_3$ les substitutions de G_4,

celles de G_{12} peuvent être rangées dans le Tableau suivant :

$$\begin{matrix} 1, & X_1, & X_2, & X_3, \\ Z_1, & Z_1X_1, & Z_1X_2, & Z_1X_3, \\ Z_2, & Z_2X_1, & Z_2X_2, & Z_2X_3. \end{matrix}$$

Puisque G_4 est un sous-groupe invariant de G_{12}, on en conclut, au moyen d'un raisonnement déjà fait (n° 84), que G_{12} se réduit, aux substitutions de G_4 près, à un groupe G_3 d'ordre 3, nécessairement cyclique. Soit $\simeq$ le symbole d'une congruence aux substitutions près de G_4, on aura

$$Z_1^3 \simeq Z_2^3 \simeq 1, \qquad Z_1^2 \simeq Z_2,$$

c'est-à-dire

$$Z_1^3 \equiv 1 \quad \text{ou} \quad Z_1^3 \equiv X_i,$$

d'où, dans tous les cas,

$$Z_1^6 \equiv 1,$$

G_{12} contient donc une substitution Z_1^2 d'ordre 3.

Posons

$$Z_1^2 = Z_3, \qquad Z_3^2 = Z_4.$$

On pourra remplacer le Tableau précédent contenant les substitutions de G_{12} par le suivant

$$\begin{matrix} 1, & X_1, & X_2, & X_3, \\ Z_3, & Z_3X_1, & Z_3X_2, & Z_3X_3, \\ Z_4, & Z_4X_1, & Z_4X_2, & Z_4X_3. \end{matrix}$$

On a

$$(Z_3X_i)^3 \simeq 1, \qquad (Z_4X_i)^3 \simeq 1, \qquad (Z_3X_i)^2 \simeq Z_4,$$

d'où

$$(Z_3X_1)^3 \equiv 1 \quad \text{ou} \quad (Z_3X_1)^3 \equiv X_h.$$

Donc, dans tous les cas,

$$[(Z_3X_1)^2]^3 \equiv 1.$$

Mais

$$(Z_3X_1)^2 \equiv Z_4X_k,$$

d'où

$$(Z_4X_h)^3 \equiv 1.$$

Cette relation peut se mettre sous une autre forme. En effet, l'élément Z_4X_h, appartenant à la troisième ligne du Tableau, est

égal au produit d'un des X, X_l, par exemple, par Z_4, en sorte qu'on peut écrire également

$$(X_l Z_4)^3 = 1.$$

Et alors les relations

$$Z_4^3 = 1, \qquad X_l^2 = 1, \qquad (X_l Z_4)^3 = 1$$

montrent (n° **104**) que le groupe G_{12} est, aux notations près, identique à $G_{(3)}$; c'est, par suite, un groupe tétraédrique.

Puisque tout groupe tétraédrique contient un seul sous-groupe trirectangle invariant, le nombre des sous-groupes tétraédriques de $G_{\mu(p)}$ est $\frac{p(p^2-1)}{24}$. Ils sont tous équivalents; il n'en existe pas d'autres (puisqu'il n'existe pas d'autres sous-groupes trirectangles).

116. Si

$$p \equiv \pm 1 \quad (\text{mod } 8),$$

un groupe trirectangle G_4 appartient à un système de $\frac{p(p^2-1)}{48}$ sous-groupes équivalents et, par suite, est permutable avec

$$\frac{p(p^2-1)}{2} : \frac{p(p^2-1)}{48} = 24 \text{ substitutions},$$

formant un groupe G_{24} qui admet G_4 comme sous-groupe invariant.

Soient

$$1, \quad X_1 = R^{\frac{p \mp 1}{4}}, \quad X_2, \quad X_3$$

les substitutions de G_4; on sait que

$$X_1 X_2 = X_3;$$

de plus, comme on l'a observé (n° **114**), les substitutions permutables avec G_4

$$1, \quad Y_1, \quad Y_2, \quad Y_3,$$

$$X_2, \qquad Y_1 X_2, \qquad Y_1^2 X_2 = X_3, \qquad Y_1^3 X_2 = Y_1 X_3,$$

où

$$Y_1 = X_1^{\frac{1}{2}} = R^{\frac{p \mp 1}{8}}$$

forment un groupe diédrique G_8 dont G_4 est un sous-groupe inva-

riant. Puisque G_8 est sous-groupe de G_{24}, on trouve, en suivant la marche habituelle, que G_{24} doit contenir une substitution Z d'ordre 3 qui, combinée avec G_4, donne un sous-groupe tétraédrique G_{12} de G_{24}. Or, G_{24} renferme deux autres sous-groupes analogues à G_8 et qu'on peut construire en prenant, au lieu de Y_1,

$$Y_2 \equiv X_2^{\frac{1}{2}} \qquad \text{ou} \qquad Y_3 \equiv X_3^{\frac{1}{2}},$$

il contient donc les neuf substitutions suivantes d'ordre 2

$$X_1, \quad X_2, \quad X_3, \quad Y_1X_2, \quad Y_1X_3, \quad Y_2X_1, \quad Y_2X_3, \quad Y_3X_1, \quad Y_3X_2.$$

D'autre part, si $Z_i (i = 1, 2, 3, \ldots, 8)$ sont les huit substitutions d'ordre 3 de G_{12}, il est impossible que les ordres des produits $Z_i Y_i^{-1}$ soient tous différents de 2, car alors il resterait au plus sept substitutions d'ordre 2, tandis que nous savons, d'autre part, qu'il y en a neuf. Indiquons par

$$Z_h Y_1^{-1} = W$$

un des produits considérés d'ordre 2, d'où

$$Z_h = WY_1.$$

Les relations

$$Y_1^4 \equiv 1, \qquad W^2 \equiv 1, \qquad (WY_1)^3 \equiv 1$$

montrent que G_{24} coïncide avec $G_{(4)}$ et est, par suite, un groupe octaédrique.

Il y a $\frac{p(p^2-1)}{24}$ groupes octaédriques, se partageant en deux systèmes de sous-groupes équivalents, et ce sont les seuls sous-groupes octaédriques.

Les sous-groupes hémimétacycliques, diédriques, tétraédriques et octaédriques trouvés ne conduisent pas à des sous-groupes plus amples, puisqu'ils ne sont permutables qu'avec leurs propres substitutions.

117. Voyons maintenant si le groupe $G_{\mu(p)}$ admet des sous-groupes icosaédriques.

Pour $p = 5$, $G_{\mu(p)}$ est le groupe icosaédrique lui-même; soit donc $p > 5$. Dans ces conditions, il faut que $\frac{p^2-1}{2}$ soit

un multiple de 5, d'où

$$p \equiv \pm 1 \qquad (\text{mod } 10).$$

Soit d'abord

$$p \equiv 1 \qquad (\text{mod } 10).$$

Alors $G_{\frac{p-1}{2}}$ contient quatre substitutions d'ordre 5

$$H = R^{\frac{p-1}{10}}, \quad H^2, \quad H^3, \quad H^4.$$

De plus, on peut trouver dans $G_{\mu(p)}$ une substitution Z d'ordre 2 telle que ZH soit d'ordre 3. En effet, posons

$$Z = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad \frac{p-1}{10} = r,$$

nous aurons

$$ZH = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a^r & 0 \\ 0 & a^{-r} \end{pmatrix} = \begin{pmatrix} \alpha a^r & \beta a^r \\ \gamma a^{-r} & \delta a^{-r} \end{pmatrix}.$$

Or Z étant d'ordre 2, et ZH d'ordre 3, on aura (n° **112**)

$$\alpha + \delta \equiv 0, \qquad \alpha a^r + \delta a^{-r} \equiv 1 \qquad (\text{mod}\, p) \quad (^1),$$

d'où

$$\alpha(a^r - a^{-r}) \equiv 1 \qquad (\text{mod}\, p),$$

relation qui détermine α, car si l'on avait

$$a^r - a^{-r} \equiv 0,$$

la substitution H se réduirait à l'identité.

On a ensuite

$$\beta\gamma \equiv -1 + \alpha\delta \equiv -1 - \alpha^2 \qquad (\text{mod}\, p),$$

d'où

$$\begin{aligned} \beta\gamma(a^r - a^{-r})^2 &\equiv -(a^r - a^{-r})^2 - \alpha^2(a^r - a^{-r})^2 \\ &\equiv -(a^r - a^{-r})^2 - 1 \\ &\equiv -[a^{2r} + a^{-2r} - 1]. \end{aligned}$$

Cette dernière expression ne peut être congrue à zéro, sinon on aurait

$$a^{2r} + a^{2r} \equiv 1 \qquad (\text{mod}\, p),$$

et alors (n° **112**) H^2 serait d'ordre 3.

---

(1) Il est inutile d'écrire ± 1 dans le second membre, puisque nous pouvons prendre arbitrairement le signe de α.

Nous obtenons ainsi pour chaque valeur arbitraire de β non divisible par p, une valeur correspondante de γ, d'où la possibilité de déterminer $p - 1$ substitutions Z, telles que

$$Z^2 \equiv 1, \qquad (ZH)^3 \equiv 1.$$

Ces relations, jointes à $H^5 \equiv 1$, montrent (n° **104**) que le sous-groupe de $G_{\mu(p)}$ engendré par les substitutions H et Z coïncide avec $G_{[5]}$, c'est donc un groupe icosaédrique.

Puisque $G_{\frac{p-1}{2}}$ contient quatre substitutions d'ordre 5, et que, pour chacune d'elles, on peut déterminer $p - 1$ substitutions d'ordre 2, on obtient $4(p-1)$ sous-groupes icosaédriques; et, en tenant compte de ce que $G_{\frac{p-1}{2}}$ appartient à un système de $\frac{p(p+1)}{2}$ sous-groupes équivalents, on conclut que le nombre total des sous-groupes icosaédriques de $G_{\mu(p)}$ est $4(p-1)\frac{p(p+1)}{2}$ ou $2p(p^2-1)$.

On arrive à la même conclusion dans le cas de

$$p \equiv -1 \pmod{10}.$$

D'ailleurs ces sous-groupes ne sont pas tous différents. Le nombre des sous-groupes distincts s'obtient en divisant $2p(p^2-1)$ par le nombre de couples de substitutions analogues à Z, H contenues dans le groupe icosaédrique. Proposons-nous de déterminer ce nombre.

Soient S la substitution modulaire qui, considérée comme appartenant au groupe icosaédrique $G_{[5]} = G_{60}$ est d'ordre 5, et

$$Z \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

une substitution d'ordre 2 du groupe icosaédrique précédent telle que ZS soit d'ordre 3.

Puisque

$$ZS \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} \alpha+\gamma & \beta+\delta \\ \gamma & \delta \end{pmatrix} \pmod 5,$$

on doit avoir (n° **112**)

$$\alpha + \delta \equiv 0, \qquad \alpha+\gamma+\delta \equiv 1 \pmod 5 \quad (^1),$$

(1) *Voir* la note de la page 185.

et en tenant compte de

$$\alpha\delta - \beta\gamma \equiv 1 \pmod 5,$$

il vient

$$\delta \equiv -\alpha, \qquad \gamma \equiv 1, \qquad \beta \equiv -1 \equiv \alpha^2 \pmod 5,$$

en sorte que α peut prendre ici cinq valeurs différentes; mais une fois fixée la valeur de α, β et γ sont déterminés, et γ est toujours congru à 1.

Donc à la substitution S correspondent cinq substitutions Z, et l'on peut en dire autant de chacune des substitutions d'ordre 5 appartenant à C_{60}. Le nombre cherché est donc

$$5 \times 24 = 120,$$

et le nombre des sous-groupes icosaédriques distincts de $G_{\mu(p)}$ est $\frac{p(p^2-1)}{60}$.

Comme nous le verrons plus loin, $G_{\mu(p)}$ n'admet aucun sous-groupe comprenant un sous-groupe icosaédrique. Il suit de là qu'un sous-groupe icosaédrique de $G_{\mu(p)}$ n'est permutable qu'avec ses propres substitutions et appartient par conséquent à un système de

$$\frac{p(p^2-1)}{2} : 60 = \frac{p(p^2-1)}{120}$$

sous-groupes équivalents.

Donc les $\frac{p(p^2-1)}{60}$ sous-groupes icosaédriques se partagent en deux systèmes de $\frac{p(p^2-1)}{120}$ sous-groupes équivalents, que nous désignerons par les notations abrégées A et B.

Puisque $G_{\mu(p)}$ admet $\frac{p(p^2-1)}{60}$ sous-groupes icosaédriques et $\frac{p(p^2-1)}{24}$ sous-groupes tétraédriques, que de plus (n° 67) chaque groupe icosaédrique comprend cinq sous-groupes tétraédriques, il y a

$$5\,\frac{p(p^2-1)}{60} : \frac{p(p^2-1)}{24} = 2$$

sous-groupes icosaédriques admettant un même sous-groupe tétraédrique.

Rappelons, aussi, que les cinq sous-groupes tétraédriques d'un groupe icosaédrique sont équivalents, que les $\frac{p(p^2-1)}{24}$ sous-groupes tétraédriques de $G_{\mu(p)}$ sont tous équivalents ou bien se partagent en deux systèmes de sous-groupes équivalents, suivant que

$$p \equiv \pm 3 \quad \text{ou} \quad p \equiv \pm 1 \pmod 8.$$

On voit alors que, dans le premier cas ($p \equiv \pm 3$), tous les $\frac{p(p^2-1)}{24}$ sous-groupes tétraédriques devront figurer dans les deux systèmes A et B, tandis que, dans le second cas ($p \equiv \pm 1$), $\frac{p(p^2-1)}{48}$ figureront dans le système A et les $\frac{p(p^2-1)}{48}$ autres dans le système B. Donc les deux sous-groupes icosaédriques qui contiennent un même sous-groupe tétraédrique ne sont pas équivalents si $p \equiv \pm 3$, et le sont au contraire si $p \equiv \pm 1 \pmod 8$.

118. Démontrons maintenant que $G_{\mu(p)}$ n'admet pas d'autres sous-groupes que les sous-groupes trouvés précédemment.

On a déjà déterminé complètement (n° 113) les sous-groupes contenant un groupe cyclique d'ordre p; on peut donc se borner aux sous-groupes G_q, ne renfermant aucun groupe cyclique d'ordre p, de sorte que q devra être un diviseur de $\frac{p^2-1}{2}$. Or, les seuls sous-groupes cycliques, dont l'ordre soit différent de p, sont d'ordre égal à $\frac{p \mp 1}{2}$ ou à un diviseur d'un de ces deux nombres. Si donc on désigne par G_{r_1} un sous-groupe cyclique de G_q qui ne soit contenu dans aucun autre sous-groupe cyclique de G_q, r_1 sera un diviseur de $\frac{p-1}{2}$ ou de $\frac{p+1}{2}$ et G_{r_1} sera le plus grand sous-groupe commun à G_q et à $G_{\frac{p \mp 1}{2}}$. Les substitutions de G_{r_1} permutables avec $G_{\frac{p \mp 1}{2}}$ comprennent, comme on l'a vu, celles du groupe lui-même et $\frac{p \mp 1}{2}$ autres substitutions d'ordre *deux*, obtenues en multipliant l'une d'elles par les substitutions de $G_{\frac{p \mp 1}{2}}$. Donc, suivant que G_q contient ou non une substitution de ce genre, permutable avec G_{r_1}, il y aura $2r_1$ ou r_1 substitutions de G_q per-

mutables avec G_{r_1}. Indiquons en général par $\sigma_1 r_1$ le nombre de telles substitutions, σ pouvant prendre les valeurs 1 et 2 ; G_{r_1} appartient à un système de $\frac{q}{\sigma_1 r_1}$ sous-groupes équivalents qui, dans leur ensemble, contiennent, outre l'identité, $\frac{(r_1-1)q}{\sigma_1 r_1}$ substitutions distinctes.

Si G_q contient encore d'autres substitutions, cherchons dans l'ensemble de ces substitutions (auxquelles nous adjoindrons l'unité) un sous-groupe G_{r_2} analogue à G_{r_1}, et poursuivons cette recherche jusqu'à ce que nous ayons considéré toutes les substitutions de G_q. Nous aurons ainsi décomposé G_q en plusieurs systèmes de sous-groupes équivalents respectivement à G_{r_1}, G_{r_2}, ..., G_{r_λ} et nous en conclurons

$$q = 1 + \sum_{i=1}^{\lambda} \frac{(r_i - 1)q}{\sigma_i r_i},$$

c'est-à-dire

$$q = \frac{1}{1 - \sum\limits_{i=1}^{\lambda} \frac{r_i - 1}{\sigma_i r_i}}. \tag{1}$$

Nous avons, d'autre part, la relation évidente

$$q \geqq \sigma_i r_i \qquad (i = 1, 2, \ldots, \lambda), \tag{2}$$

car G_q devant contenir $\sigma_i r_i$ substitutions permutables avec G_{r_i}, ne peut être d'ordre inférieur à $\sigma_i r_i$.

On obtient enfin une troisième relation de la façon suivante. Soient G_{r_h}, G_{r_k} des groupes d'ordre impair, X_h, X_k leurs substitutions génératrices. Les sous-groupes

$$X_k^{-s} G_{r_h} X_k^s \qquad (s = 0, 1, 2, \ldots, r_k - 1)$$

sont tous distincts. En effet, G_{r_h} n'est permutable qu'avec ses propres substitutions, et avec des substitutions d'ordre pair. Or X_k, appartenant à un groupe G_{r_k} d'ordre impair, ne peut être d'ordre pair.

De même, les sous-groupes

$$X_h^{-s} G_{r_k} X_h^s$$

sont tous distincts et ils n'ont évidemment aucun élément commun

avec les sous-groupes précédents. Or les premiers sous-groupes contiennent, outre l'identité, $r_k(r_h - 1)$ substitutions, et les seconds en contiennent $r_h(r_k - 1)$. On a donc *pour chaque couple de nombres impairs* r_h, r_k

$$q \geqq 1 + r_k(r_h - 1) + r_h(r_k - 1),$$

c'est-à-dire

$$(3) \qquad q \geqq 2 r_h r_k - r_h - r_k + 1.$$

119. L'étude des relations (1), (2), (3) va nous conduire au résultat cherché.

Tout d'abord, les coefficients σ_i étant égaux à 1 ou à 2, on a

$$\frac{r_i - 1}{\sigma_i r_i} \geqq \frac{r_i - 1}{2 r_i} \geqq \frac{1}{4},$$

et comme dans le second nombre de (1) le dénominateur doit être positif, on a $\lambda \leqq 3$, d'où trois cas à examiner : $\lambda = 1$, $\lambda = 2$, $\lambda = 3$, Soit d'abord $\lambda = 1$. Les relations (1) et (2) deviennent

$$q = \frac{1}{1 - \frac{r_1 - 1}{\sigma_1 r_1}} = \frac{\sigma_1 r_1}{\sigma_1 r_1 - r_1 + 1}, \qquad q \geqq \sigma_1 r_1$$

et, par conséquent,

$$\sigma_1 r_1 - r_1 + 1 \leqq 1$$

ou bien

$$(\sigma_1 - 1) r_1 \leqq 0,$$

d'où

$$\sigma_1 - 1 \leqq 0$$

et, par suite,

$$\sigma_1 = 1, \qquad q = r_1.$$

Soit maintenant $\lambda = 2$. La relation (1) donne

$$q = \frac{1}{1 - \frac{r_1 - 1}{\sigma_1 r_1} - \frac{r_2 - 1}{\sigma_2 r_2}}.$$

Pour $\sigma_1 = \sigma_2 = 2$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{2 r_1} - \frac{r_2 - 1}{2 r_2}} = \frac{2 r_1 r_2}{r_1 + r_2} < 2 r_1 = \sigma_1 r_1,$$

relation en contradiction avec l'inégalité (2).

Pour $\sigma_1 = 2$, $\sigma_2 = 1$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{2r_1} - \frac{r_2 - 1}{2r_2}} = \frac{2}{\frac{1}{r_1} + \frac{2}{r_2} - 1},$$

ce qui exige qu'on ait

$$\frac{1}{r_1} + \frac{2}{r_2} > 1.$$

Puisque $r_1 > 1$, on doit avoir $r_2 < 4$, d'où $r_2 = 2$ ou $r_2 = 3$. Si $r_2 = 2$, r_1 peut prendre une valeur quelconque, et il en résulte que $q = 2r_1$. Si $r_2 = 3$, on a nécessairement $r_1 = 2$, d'où $q = 12$.

Dans les deux cas, l'inégalité (2) est satisfaite.

Quant à l'inégalité (3), il n'y a pas lieu de s'en servir puisque l'une des quantités r est paire.

Enfin, pour $\sigma_1 = \sigma_2 = 1$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{r_1} - \frac{r_2 - 1}{r_2}} = \frac{1}{\frac{1}{r_1} + \frac{1}{r_2} - 1},$$

d'où nécessairement

$$\frac{1}{r_1} + \frac{1}{r_2} > 1,$$

ce qui est impossible, puisque r_1 et r_2 sont au moins égaux à 2.

Soit enfin $\lambda = 3$; alors

$$q = \frac{1}{1 - \frac{r_1 - 1}{\sigma_1 r_1} - \frac{r_2 - 1}{\sigma_2 r_2} - \frac{r_3 - 1}{\sigma_3 r_3}}.$$

Pour $\sigma_1 = \sigma_2 = \sigma_3 = 2$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{2r_1} - \frac{r_2 - 1}{2r_2} - \frac{r_3 - 1}{2r_3}} = \frac{2}{\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1},$$

c'est-à-dire

$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} = 1 + \frac{2}{q}.$$

C'est la relation (2) du paragraphe 37, où n est remplacé par q,

et dont on a déterminé les solutions qui sont les suivantes :

$$\begin{array}{llll} r_1 = 2, & r_2 = 2, & r_3 \text{ quelconque}, & q = 2r_3, \\ r_1 = 2, & r_2 = 3, & r_3 = 3, & q = 12, \\ r_1 = 2, & r_2 = 3, & r_3 = 4, & q = 24, \\ r_1 = 2, & r_2 = 3. & r_3 = 5, & q = 60. \end{array}$$

Il est facile de vérifier que l'inégalité (2) est toujours satisfaite; quant à l'inégalité (3) elle n'est pas satisfaite pour $h = 2$, $k = 3$, et par suite la solution $r_1 = 2$, $r_2 = 3$, $r_3 = 3$, $q = 12$ est à rejeter.

Pour $\sigma_1 = \sigma_2 = 2$, $\sigma_3 = 1$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{2r_1} - \frac{r_2 - 1}{2r_2} - \frac{r_3 - r_1}{r_3}} = \frac{1}{\frac{1}{2r_1} + \frac{1}{2r_2} + \frac{1}{r_3} - 1}$$

et comme

$$\frac{1}{2r_1} + \frac{1}{2r_2} + \frac{1}{r_3} - 1 \leqq \frac{1}{4} + \frac{1}{4} + \frac{1}{2} - 1 = 0,$$

q serait infini ou négatif.

Pour $\sigma_1 = 2$, $\sigma_2 = \sigma_3 = 1$,

$$q = \frac{1}{1 - \frac{r_1 - 1}{2r_1} - \frac{r_2 - 1}{r_2} - \frac{r_3 - 1}{r_3}} = \frac{1}{\frac{1}{2r_1} + \frac{1}{r_2} + \frac{1}{r_3} - \frac{3}{2}}$$

et comme

$$\frac{1}{2r_1} + \frac{1}{r_2} + \frac{1}{r_3} - \frac{3}{2} \leqq \frac{1}{4} + \frac{1}{2} + \frac{1}{2} - \frac{3}{2} = -\frac{1}{4} < 0,$$

q serait négatif.

Enfin, pour $\sigma_1 = \sigma_2 = \sigma_3 = 1$, on a

$$q = \frac{1}{1 - \frac{r_1 - 1}{r_1} - \frac{r_2 - 1}{r_2} - \frac{r_3 - 1}{r_3}} = \frac{1}{\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 2},$$

mais

$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 2 \leqq \frac{3}{2} - 2 = -\frac{1}{2} < 0$$

et q serait négatif.

En résumé, on a, pour les solutions du système,

(a) $\lambda = 1, \quad \sigma_1 = 1, \quad r_1$ quelconque, $\quad q = r_1,$

(b) $\begin{cases} \lambda = 2, \quad \sigma_1 = 2, \quad \sigma_2 = 1, \quad r \text{ quelconque}, \\ r_1 \text{ quelconque}, \quad r_2 = 2, \quad q = 2r_1, \end{cases}$

(c) $\lambda = 2, \quad \sigma_1 = 2, \quad \sigma_2 = 1, \quad r_1 = 2, \quad r_2 = 3, \quad q = 12,$

(d) $\begin{cases} \lambda = 3, \quad \sigma_1 = \sigma_2 = \sigma_3 = 2, \quad r_1 = 2, \quad r_2 = 2, \\ r_3 \text{ quelconque}, \quad q = 2r_3, \end{cases}$

(e) $\lambda = 3, \quad \sigma_1 = \sigma_2 = \sigma_3 = 2, \quad r_1 = 2, \quad r_2 = 3, \quad r_3 = 4, \quad q = 24,$

(f) $\lambda = 3, \quad \sigma_1 = \sigma_2 = \sigma_3 = 2, \quad r_1 = 2, \quad r_2 = 3, \quad r_3 = 5, \quad q = 60.$

120. Voyons quelle est la signification de ces solutions.

La solution (*a*) représente évidemment des groupes cycliques.

Les solutions (*b*) et (*d*) représentent des groupes diédriques, la première pour $\frac{q}{2}$ impair, la seconde pour $\frac{q}{2}$ pair. En effet, dans le premier cas, les sous-groupes du second ordre sont tous équivalents, et chacun d'eux n'est permutable qu'avec ses propres substitutions ($\sigma_2 = 1$). Dans le second cas, ils se partagent en deux systèmes de sous-groupes équivalents [1]; chacun d'eux est permutable avec ses propres substitutions et avec deux autres ($\sigma_2 = 2, \sigma_3 = 2$); correspondant respectivement aux deux rotations d'ordre 2 autour de l'axe polaire et de l'axe équatorial perpendiculaire à l'axe de la rotation non nulle de ce sous-groupe.

La solution (*c*) représente un groupe tétraédrique. En effet, le groupe correspondant contient un sous-groupe d'ordre 3 permutable avec ses propres substitutions ($r_2 = 3, \sigma_2 = 1$) et appartenant par conséquent à un système de $\frac{12}{3} = 4$ sous-groupes équivalents. Ces sous-groupes contiennent en tout huit substitutions d'ordre 3. Les trois substitutions restantes (outre l'identité) sont d'ordre 2 ($r_1 = 2$) et permutables entre elles ($\sigma_1 = 2$); elles forment donc avec l'identité un groupe trirectangle qui, étant unique, est nécessairement invariant. Il suit de là (*cf.* n° 115) que le groupe considéré est tétraédrique.

La solution (*e*) représente un groupe octaédrique. En effet, le

(1) Ces sous-groupes se composent de la rotation nulle et d'une rotation π autour d'un axe. Ces axes sont tous situés dans le plan équatorial du dièdre.

groupe correspondant contient tout d'abord $\frac{q}{\sigma_3 r_3} = 3$ sous-groupes cycliques d'ordre 4 équivalents G_4, G'_4, G''_4. Soient Y, Y', Y'' leurs substitutions génératrices, on a

$$Y^{-1} G'_4 Y = G'_4, \qquad Y^{-1} G''_4 Y = G''_4$$

et aussi

$$Y^{-1} G'_4 Y = G''_4, \qquad Y^{-1} G''_4 Y = G'_4.$$

Donc, dans tous les cas,

$$Y^{-2} G'_4 Y^2 = G'_4, \qquad Y^{-2} G''_4 Y^2 = G''_4,$$

et, puisqu'une substitution et sa transformée sont du même ordre

$$Y^{-2} Y'^2 Y^2 = Y'^2, \qquad Y^{-2} Y''^2 Y^2 = Y''^2,$$

on aura de même

$$Y'^{-2} Y''^2 Y'^2 = Y''^2.$$

Le groupe contient donc trois substitutions d'ordre 2, permutables entre elles, Y^2, Y'^2, Y''^2 qui, avec l'identité, forment un sous-groupe trirectangle. De plus, comme les sous-groupes G_4, G'_4, G''_4 forment un système complet de sous-groupes équivalents, les substitutions Y^2, Y'^2, Y''^2 sont équivalentes entre elles et le sous-groupe trirectangle auquel elles appartiennent est invariant. Il résulte de là (*cf.* n° 116) que le groupe considéré est octaédrique.

Enfin, la solution (f) représente un groupe icosaédrique.

Le groupe G_{60}, défini par f, contient $\frac{q}{\sigma_1 r_1} = 15$ groupes G_2 équivalents ($\sigma_1 = 2$, $r_1 = 2$), $\frac{q}{\sigma_2 r_2} = 10$ groupes G_3 équivalents ($\sigma_2 = 2$, $r_2 = 3$), et $\frac{q}{\sigma_3 r_3} = 6$ groupes G_5 équivalents ($\sigma_3 = 2$, $r_3 = 5$). Soient $X_1, X_2, \ldots, X_{15}$ les quinze substitutions d'ordre 2, et soit Y une substitution d'ordre 3. Considérons un des produits $X_i Y$, et supposons d'abord qu'il représente une substitution d'ordre 2. Posons

$$X_i Y \equiv X_h,$$

d'où

$$Y \equiv X_i^{-1} X_h \equiv X_i X_h.$$

Les trois relations

$$X_h^2 \equiv 1, \qquad X_i^2 \equiv 1, \qquad (X_i X_h)^3 \equiv 1$$

montrent (n° 104) que les X_i et X_h ou, ce qui revient au même, les X_i et Y engendrent un groupe diédrique G_6 d'ordre 6. Or, σ_2 étant égal à 2, chaque sous-groupe G_3 est lui-même sous-groupe invariant d'un sous-groupe diédrique G_6 de G_{60}, et par conséquent G_{60} renferme dix sous-groupes diédriques d'ordre 6.

Parmi les substitutions de ces derniers sous-groupes pris dans leur ensemble figurent vingt substitutions d'ordre 3, et comme dans le groupe G_{60} il y a précisément vingt substitutions d'ordre 3, on en conclut que chacune de ces substitutions figure dans un seul des groupes G_6. D'autre part, chacun des G_6 contient trois substitutions d'ordre 2; donc, à chaque substitution Y d'ordre 3 correspondent trois produits $X_i Y$ d'ordre 2.

Supposons au contraire $X_i Y$ d'ordre 3, alors

$$Y^3 \equiv 1, \qquad X_i^2 \equiv 1, \qquad (X_i Y)^3 \equiv 1,$$

les Y, X_i engendrent (n° 104) un groupe tétraédrique. Puisque chaque groupe G_2 est permutable avec deux autres substitutions d'ordre 2 ($\sigma_1 = 2$), les 15 groupes G_2 se partagent en 5 systèmes de 3 substitutions, les substitutions de chaque système étant permutables entre elles. Nous aurons donc 5 groupes trirectangles, et, par suite, 5 groupes tétraédriques. Ces derniers comprennent en tout 40 substitutions d'ordre 3, et, puisque les substitutions de cet ordre sont au nombre de 20, chacune d'elles figurera dans deux groupes tétraédriques. D'autre part, chaque groupe tétraédrique contient 3 opérations d'ordre 2; donc à chaque substitution Y d'ordre 3 correspondent 6 produits $X_i Y$ d'ordre 3.

Les 6 produits restants $X_i Y$ seront nécessairement d'ordre 5. Soit Z l'un d'eux, on a

$$Z \equiv X_i Y, \qquad Y = X_i^{-1} Z \equiv X_i Z,$$

et les relations

$$Z^5 \equiv 1, \qquad X_i^2 \equiv 1, \qquad (X_i Z)^3 \equiv 1$$

montrent que les substitutions Z, X_i, ou bien encore X_i, Y engendrent un groupe icosaédrique.

Donc notre groupe G_{60} contient un sous-groupe icosaédrique; or, tout groupe icosaédrique étant d'ordre 60, G_{60} est lui-même un groupe icosaédrique.

On voit donc bien que $G_{\mu(p)}$ n'admet pas d'autres sous-groupes que les sous-groupes cycliques, hémimétacycliques, diédriques, octaédriques et icosaédriques.

Et comme chacun des sous-groupes trouvés est invariant, on en conclut encore que, *si p est un nombre premier*, $G_{\mu(p)}$ *est un groupe simple*.

DEUXIÈME PARTIE.

LES FONCTIONS ET LES ÉQUATIONS POLYÉDRIQUES ET MODUDAIRES.

Formes et fonctions polyédriques et modulaires.

121. On dit qu'une forme algébrique binaire est *invariante* pour une substitution linéaire, si la substitution a pour effet de laisser la forme inaltérée ou de la multiplier par un facteur constant. Dans le premier cas, on dit aussi que la forme est *absolument invariante*.

On dit qu'une forme est invariante dans un groupe de substitutions linéaires et homogènes, si elle est invariante pour toutes les substitutions de ce groupe.

Il est évident qu'une forme est invariante pour une substitution, si cette substitution a pour effet de ne rien changer aux racines de la forme ou de les échanger entre elles, et ce sont les deux seuls cas possibles. Il suit de là qu'*une forme n'est invariante dans un groupe fini de substitutions homogènes* G'_{2n}, *que si elle admet pour racines un ou plusieurs systèmes de points homologues relativement au groupe correspondant* G_n *de substitutions non homogènes*.

On appelle *formes invariantes fondamentales* relatives à un groupe homogène G'_{2n} ou au groupe non homogène correspondant G_n, celles dont les racines constituent un système unique de points homologues. Toute forme invariante est un produit de formes fondamentales. Les formes fondamentales au nombre de deux pour les groupes cycliques, de trois pour les groupes polyédriques, sont de degré n (n° 80). Ce sont des puissances d'ordre ν_i des formes de degré $\frac{n}{\nu_i}$, dont les racines sont des nœuds du réseau,

et on les désigne spécialement sous le nom de *formes fondamentales simples*.

Pour construire le type le plus général des formes fondamentales correspondant à chaque groupe fini, nous utiliserons la remarque suivante :

Une forme fondamentale est tout à fait déterminée, si l'on se donne une de ses racines, par suite l'expression la plus générale d'une forme fondamentale contient un seul paramètre arbitraire.

Nous construirons donc pour chaque groupe les formes fondamentales simples, nous en déduirons une forme invariante de degré n contenant un paramètre arbitraire, et nous aurons ainsi la forme fondamentale la plus générale invariante dans le groupe considéré.

122. L'application des considérations précédentes aux groupes cycliques est immédiate.

Il y a, dans ce cas, deux systèmes de nœuds formés chacun d'un seul nœud d'ordre n et situés respectivement à l'origine et au point à l'infini. En désignant par (z_1, z_2) le point $\frac{z_1}{z_2}$, ces nœuds sont représentés par $(1, 0)$ $(0, 1)$. Donc les deux formes simples sont

$$\Phi_1 = F_1^n = z_1^n, \qquad \Phi_2 = F_2^n = z_2^n.$$

Soient Φ'_i, F'_i les mêmes formes où z_1, z_2 ont été remplacés par z'_1, z'_2

$$\Phi'_1 = F_1'^n = z_1'^n, \qquad \Phi'_2 = F_2'^n = z_2'^n.$$

Appliquant les substitutions (n° **71**)

$$z'_1 = e^{\frac{h\pi i}{n}} z_1, \qquad z'_2 = e^{-\frac{h\pi i}{n}} z_2 \qquad (h = 0, 1, 2, \ldots, 2n-1),$$

du groupe cyclique homogène, nous trouvons

$$\Phi'_1 = F_1'^n = (-1)^h z_1^n = (-1)^h \Phi_1 = (-1)^h F_1^n,$$
$$\Phi'_2 = F_2'^n = (-1)^h z_2^n = (-1)^h \Phi_2 = (-1)^h F_2^n,$$

Posant ensuite

$$(1) \qquad F = \lambda_1 F_1^n + \lambda_2 F_2^n,$$

on aura, quel que soit $\frac{\lambda_1}{\lambda_2}$,

$$F' = (-1)^h F.$$

Donc (1) qui est une forme invariante contenant un seul paramètre représente la forme fondamentale la plus générale pour le groupe cyclique considéré.

123. Avant de passer aux groupes polyédriques, développons quelques considérations préliminaires.

Étant donné un groupe polyédrique, les nœuds du réseau correspondant se partagent en trois systèmes de points homologues, auxquels correspondent respectivement trois formes simples $F_1^{\nu_1}$, $F_2^{\nu_2}$, $F_3^{\nu_3}$; F_1, F_2, F_3 désignant des formes de degrés $\frac{n}{\nu_1}$, $\frac{n}{\nu_2}$, $\frac{n}{\nu_3}$. Si, comme cela a lieu effectivement dans tous les cas que nous rencontrerons, une substitution du groupe a pour effet de multiplier chacune de ces trois formes par le même facteur, l'expression

$$F = \lambda_1 F_1^{\nu_1} + \lambda_2 F_2^{\nu_2} + \lambda_3 F_3^{\nu_3}$$

sera une forme invariante fondamentale, quelles que soient les valeurs de λ_1, λ_2, λ_3. Mais la forme fondamentale la plus générale contenant un seul paramètre, les fonctions $F_1^{\nu_1}$, $F_2^{\nu_2}$, $F_3^{\nu_3}$ ne peuvent être linéairement indépendantes, c'est-à-dire qu'il doit exister entre elles une relation linéaire et homogène à coefficients constants

$$(1) \qquad \mu_1 F_1^{\nu_1} + \mu_2 F_2^{\nu_2} + \mu_3 F_3^{\nu_3} = 0.$$

En tenant compte de cette relation, F se réduit à

$$F = \frac{1}{\mu_1}[(\lambda_1\mu_3 - \lambda_3\mu_1)F_1 + (\lambda_2\mu_3 - \lambda_3\mu_2)F_2] = \lambda'_1 F_1 + \lambda'_2 F_2,$$

et dans cette expression figure un seul paramètre.

Nous construirons pour chaque groupe polyédrique les formes F_1, F_2, F_3; nous établirons la relation (1) correspondante et nous trouverons que dans tous les cas une des trois formes est le déterminant fonctionnel des deux autres.

124. Les nœuds du réseau diédrique ($n = 2m$) sont les m som-

mets du polygone équatorial, les m points milieux des arcs sous-tendus par les côtés et les deux pôles. Puisque les sommets du polygone divisent l'équateur en m parties égales. Puisque le polygone régulier a m côtés et que l'un des sommets est situé au point $z = 1$, les valeurs de z correspondantes seront les racines de l'équation binome

$$z^m - 1 = 0.$$

Le second ensemble de points divise aussi l'équateur en m parties égales, et comme l'un d'eux est $z = e^{\frac{\pi i}{m}}$, les m valeurs de z correspondantes sont racines de l'équation

$$z^m - \left(e^{\frac{\pi i}{m}}\right)^m = z^m + 1 = 0.$$

En coordonnées homogènes, les deux équations deviennent

$$z_1^m - z_2^m = 0, \qquad z_1^m + z_2^m = 0.$$

De plus l'équation dont les racines sont les deux pôles de la sphère est

$$z_1 z_2 = 0.$$

Donc, on a pour les trois formes cherchées

$$F_1 = \frac{1}{2}(z_1^m - z_2^m), \qquad F_2 = \frac{1}{2}(z_1^m + z_2^m), \qquad F_3 = z_1 z_2.$$

Voyons comment varient ces formes par les substitutions du groupe diédrique (n° 71)

$$\left.\begin{array}{lll} (a) & z'_1 = e^{\frac{h\pi i}{m}} z_1, & z'_2 = e^{-\frac{h\pi i}{m}} z_2 \\ (b) & z'_1 = i\,e^{\frac{h\pi i}{m}} z_2, & z'_2 = i\,e^{-\frac{h\pi i}{m}} z_1 \end{array}\right\} \qquad (h = 0, 1, 2, \ldots, 2m-1).$$

La substitution a nous donne

$$F'_1 = \frac{1}{2}(z_1'^m - z_2'^m) = \frac{1}{2}(-1)^h(z_1^m - z_2^m) = (-1)^h F_1,$$

$$F'_2 = \frac{1}{2}(z_1'^m - z_2'^m) = \frac{1}{2}(-1)^h(z_1^m - z_2^m) = (-1)^h F_2,$$

$$F'_3 = \qquad z'_1 z'_2 \qquad = \qquad z_1 z_2 \qquad = F_3,$$

d'où

$$F_1'^2 = F_1^2, \qquad F_2'^2 = F_2^2, \qquad F_3'^m = F_3^m.$$

Pour la substitution b, on a

$$F'_1 = \frac{1}{2}(z'^m_1 - z'^m_2) = \frac{1}{2} i^m (-1)^h (z^m_2 - z^m_1) = - i^m (-1)^h F_1,$$

$$F'_2 = \frac{1}{2}(z'^m_1 + z'^m_2) = \frac{1}{2} i^m (-1)^h (z^m_1 + z^m_2) = \quad i^m (-1)^h F_2,$$

$$F'_3 = \qquad z'_1 z'_2 \qquad = \qquad - z_1 z_2 \qquad = - F_3,$$

d'où

$$F'^2_1 = (-1)^m F^2_1, \qquad F'^2_2 = (-1)^m F^2_2, \qquad F'^m_3 = (-1)^m F^m_3.$$

Les formes Φ_1, Φ_2, Φ_3, pour chaque substitution sont donc chacune multipliées par le même facteur, et l'on a pour type général de la forme fondamentale

$$F = \lambda_1 F^2_1 + \lambda_2 F^2_2 + \lambda_3 F^m_3 = \lambda_1 \left(\frac{z^m_1 - z^m_2}{2}\right)^2 + \lambda_2 \left(\frac{z^m_1 + z^m_2}{2}\right)^2 + \lambda_3 (z_1 z_2)^m.$$

La relation (1) du n° 123 devient ici

$$\mu_1 \left(\frac{z^m_1 - z^m_2}{2}\right)^2 + \mu_2 \left(\frac{z^m_1 + z^m_2}{2}\right)^2 + \mu_3 (z_1 z_2)^m = 0.$$

Développons, il vient

$$\frac{\mu_1 + \mu_2}{4} z^{2m}_1 + \left(- \frac{\mu_1 - \mu_2}{2} + \mu_1\right) z^m_1 z^m_2 + \frac{\mu_1 + \mu_2}{4} z^{2m}_2 = 0,$$

d'où

$$\frac{\mu_1 + \mu_2}{4} = 0, \qquad \frac{\mu_1 - \mu_2}{2} + \mu_3 = 0,$$

par suite

$$\mu_1 : \mu_2 : \mu_3 = 1 : -1 : 1,$$

en sorte que la relation cherchée est

$$F^2_1 - F^2_2 + F^m_3 = 0.$$

On peut vérifier que F_1 est, à un facteur constant près, le déterminant fonctionnel de F_2 et F_3. Si l'on représente par $J(\varphi, \psi)$ le déterminant fonctionnel ou jacobien des deux fonctions de deux variables φ, ψ, on a

$$J(F_2, F_1) = \begin{vmatrix} \frac{m}{2} z^{m-1}_1 & \frac{m}{2} z^{m-1}_2 \\ z_2 & z_1 \end{vmatrix} = \frac{m}{2}(z^m_1 - z^m_2) = m F_1.$$

125. Les nœuds du réseau tétraédrique sont les 6 milieux des arêtes, les 4 centres des faces et les 4 sommets du tétraèdre sphérique.

Les premiers sont les intersections des trois axes de coordonnées avec la sphère de rayon 1, c'est-à-dire les points

$$z = 1,\ -1,\ i,\ -i,\ 0,\ \infty.$$

Par suite la forme correspondante est

$$F_1 = (z_1 - z_2)(z_1 + z_2)(z_1 - i z_2)(z_1 + i z_2) z_1 z_2 = z_1 z_2 (z_1^4 - z_2^4).$$

Nous la désignerons par t.

Les points du deuxième et du troisième ensemble constituent les sommets du cube rencontré dans la théorie du tétraèdre. Les coordonnées de ces sommets ont tous (n° 63) pour valeur absolue $\frac{1}{\sqrt{3}}$ et s'obtiennent en prenant toutes les combinaisons possibles de signes. On voit facilement que, dans la disposition adoptée précédemment (voir *fig.* 5), on a pour les coordonnées des centres des faces (ou bien encore des sommets du tétraèdre polaire)

$$A'\left(-\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}}\right),$$

$$B'\left(-\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}}\right),$$

$$C'\left(\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}}\right),$$

$$D'\left(\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}}\right)$$

et pour les coordonnées des sommets

$$A\left(\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}}\right),$$

$$B\left(\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}}\right),$$

$$C\left(-\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}}\right),$$

$$D\left(-\frac{1}{\sqrt{3}},\quad -\frac{1}{\sqrt{3}},\quad \frac{1}{\sqrt{3}}\right).$$

Les valeurs correspondantes de z se calculent à l'aide des formules (4) (n° 3). On obtient ainsi (δ et ε pouvant prendre indépendamment l'un de l'autre les valeurs $+1$ et -1), pour les centres des faces,

$$z = \delta \frac{1 + \varepsilon i}{\sqrt{3} + \varepsilon}$$

et pour les sommets

$$z = \delta \frac{1 + \varepsilon i}{\sqrt{3} + \varepsilon}.$$

Les formes F_2, F_3 qui s'annulent en ces points sont

$$F_2 = z_1^4 + 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4,$$
$$F_3 = z_1^4 - 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4,$$

nous les représenterons respectivement par φ et ψ.

En résumé les trois formes simples sont

$$F_1 = t = z_1 z_2 (z_1^4 - z_2^4),$$
$$F_2 = \varphi = z_1^4 + 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4,$$
$$F_3 = \psi = z_1^4 - 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4.$$

Il est intéressant d'avoir également l'expression de ces formes à l'aide des variables $\mathbf{z}_1$, $\mathbf{z}_2$ liées par la relation $\frac{\mathbf{z}_1}{\mathbf{z}_2} = \mathbf{z}$ à la variable $\mathbf{z}$ employée à la fin du n° 63. La première des relations (5) (n° 63) permet de poser

$$z_1 = \frac{1+i}{\sqrt{2}} \mathbf{z}_1, \qquad z_2 = \mathbf{z}_2,$$

on obtient ainsi

$$t = -\frac{1+i}{\sqrt{2}} \mathbf{z}_1 \mathbf{z}_2 (\mathbf{z}_1^4 + \mathbf{z}_2^4),$$
$$\varphi = -(\mathbf{z}_1^4 + 2\sqrt{3}\, \mathbf{z}_1^2 \mathbf{z}_2^2 - \mathbf{z}_2^4),$$
$$\psi = -(\mathbf{z}_1^4 - 2\sqrt{3}\, \mathbf{z}_1^2 \mathbf{z}_2^2 - \mathbf{z}_2^4),$$

formes auxquelles on peut substituer les suivantes :

$$\mathbf{t} = \mathbf{z}_1 \mathbf{z}_2 (\mathbf{z}_1^4 + \mathbf{z}_2^4) = -\frac{1-i}{\sqrt{2}} t,$$
$$\Phi = \mathbf{z}_1^4 + 2\sqrt{3}\, \mathbf{z}_1^2 \mathbf{z}_2^2 - \mathbf{z}_2^4 = -\varphi,$$
$$\Psi = \mathbf{z}_1^4 - 2\sqrt{3}\, \mathbf{z}_1^2 \mathbf{z}_2^2 - \mathbf{z}_2^4 = -\psi.$$

Les substitutions du groupe tétraédrique sont :

1° Les substitutions d'un sous-groupe trirectangulaire, à savoir :

$$(a) \qquad z_1' = i^h z_1, \qquad z_2' = i^{-h} z_2,$$

$$(b) \qquad z_1' = i^h z_3, \qquad z_2' = -i^{-h} z_1;$$

2° Celles qu'on obtient, en combinant ces dernières avec la substitution

$$(c) \qquad z_1' = \alpha z_1 - \beta z_2, \qquad z_2' = \alpha z_1 + \beta z_2,$$

ou avec son carré

$$\left(\alpha = \frac{1+i}{2},\ \beta = \frac{1-i}{2}\right).$$

Pour la substitution (a) on a

$$z_1'^4 = z_1^4, \qquad z_1' z_2' = z_1 z_2, \qquad z_1'^4 = z^4,$$

d'où

$$t' = z_1' z_2'(z_1'^4 - z_2'^4) = z_1 z_2(z_1^4 - z_2^4) = t,$$

$$\varphi' = z_1'^4 + 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = z_1^4 + 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4 = \varphi,$$

$$\psi' = z_1'^4 - 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = z_1^4 - 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4 = \psi.$$

Pour la substitution (b) on a

$$z_1'^4 = z_2^4, \qquad z_1' z_2' = -z_1 z_2, \qquad z_2'^4 = z_1^4,$$

d'où

$$t' = z_1' z_2'(z_1^4 - z_2^4) = -z_1 z_2(z_2^4 - z_1^4) = t,$$

$$\varphi' = z_1'^4 + 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = z_2^4 + 2i\sqrt{3}\, z_2^2 z_1^2 + z_1^4 = \varphi,$$

$$\psi' = z_1'^4 - 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = z_2^4 - 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4 = \psi.$$

Pour la substitution (c) on a

$$z_1'^4 + z_2'^4 = -\frac{1}{2} z_1^4 + 3 z_1^2 z_2^2 - \frac{1}{2} z_2^4,$$

$$z_1'^4 - z_2'^4 = -2i z_1 z_2(z_1^2 - z_2^2),$$

$$z_1' z_2' = -2i z_1 z_2(z_1^2 - z_2^2),$$

d'où

$$t' = z_1' z_2'(z_1'^4 - z_2'^4) = z_1 z_2(z_1^4 - z_2^4) = t,$$

$$\varphi' = z_1'^4 + 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = -\frac{1+i\sqrt{3}}{2}(z_1^4 + 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4) = -\frac{1+i\sqrt{3}}{2}\varphi,$$

$$\psi' = z_1'^4 - 2i\sqrt{3}\, z_1'^2 z_2'^2 + z_2'^4 = -\frac{1-i\sqrt{3}}{2}(z_1^4 - 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^2) = -\frac{1-i\sqrt{3}}{2}\psi.$$

On a donc, dans tous les cas,

$$t'^2 = t^2, \qquad \varphi'^3 = \varphi^3, \qquad \psi'^3 = \psi^3,$$

et le type général des forces fondamentales des groupes tétraédriques est

$$F = \lambda_1 t^2 + \lambda_2 \varphi^3 + \lambda_3 \psi^3.$$

La relation linéaire devient ici

$$\mu_1 t^2 + \mu_2 \varphi^3 + \mu_3 \psi^3 = 0.$$

Pour en déterminer les coefficients, il suffit de développer le premier membre et d'égaler à zéro les coefficients de deux des termes du développement. On a

$$\mu_1(z_1^{10} z_2^2 - \ldots) + \mu_2(z_1^{12} + 6i\sqrt{3}\, z_1^{10} z_2^2 + \ldots) + \mu_3(z_1^{12} - 6i\sqrt{3}\, z_1^{10} z_2^2 + \ldots) = 0,$$

d'où

$$\mu_2 + \mu_3 = 0, \qquad \mu_1 + 6i\sqrt{3}\,(\mu_2 - \mu_3) = 0,$$

ou bien

$$\mu_1 : \mu_2 : \mu_3 = 12i\sqrt{3} : -1 : 1.$$

La relation cherchée est donc

$$12i\sqrt{3}\, t^2 - \varphi^3 + \psi^3 = 0.$$

Elle devient, avec le second système de coordonnées,

$$12\sqrt{3}\, \mathbf{t}^2 - \Phi^3 + \Psi^3 = 0.$$

Vérifions que t est le déterminant fonctionnel de φ, ψ. On a, en effet,

$$J(\varphi, \psi) = \begin{vmatrix} 4z_1^3 + 4i\sqrt{3}\, z_1 z_2^2 & 4i\sqrt{3}\, z_1^2 z_2 + 4z_2^3 \\ 4z_1^3 - 4i\sqrt{3}\, z_1 z_2^2 & -4i\sqrt{3}\, z_1^2 z_2 + 4z_3^3 \end{vmatrix} = -32i\sqrt{3}\, t.$$

On peut encore observer que ψ est le hessien de φ. En effet

$$H(\varphi) = \begin{vmatrix} 12z_1^2 + 4i\sqrt{3}\, z_2^2 & 8i\sqrt{3}\, z_1 z_2 \\ 8i\sqrt{3}\, z_1 z_2 & 4i\sqrt{3}\, z_1^2 + 12z_2^2 \end{vmatrix} = 48i\sqrt{3}\, \psi.$$

126. Les nœuds du réseau octaédrique sont les milieux des 12 arêtes, les centres des 8 faces et les 6 sommets. Ces derniers sont les racines de t et les centres des 8 faces sont les sommets des

deux tétraèdres polaires; on a, par suite,

$$F_3 = t, \qquad F_2 = \varphi\psi = W,$$

W désignant le produit $\varphi\psi$. Les milieux des arêtes ont une coordonnée nulle; les deux autres coordonnées ont pour valeurs $\pm\frac{1}{\sqrt{2}}$, de sorte que, en posant $\frac{1}{\sqrt{2}} = \rho$, les coordonnées des milieux des arêtes ont pour expression

$$\begin{array}{llll}(0, \rho, \rho), & (0, \rho, -\rho), & (0, -\rho, -\rho), & (0, -\rho, \rho),\\ (\rho, 0, 0), & (\rho, 0, -\rho), & (-\rho, 0, -\rho), & (-\rho, 0, \rho),\\ (\rho, \rho, 0), & (\rho, -\rho, 0), & (-\rho, -\rho, 0), & (-\rho, \rho, 0).\end{array}$$

En désignant par δ et ε deux quantités pouvant prendre indépendamment l'une de l'autre les valeurs $+1$ et -1, on a, pour les valeurs correspondantes de z,

$$z = \frac{\delta i \rho}{1+\varepsilon\rho}, \qquad z = \frac{\delta\rho}{1+\varepsilon\rho}, \qquad z = \delta\rho(1+\varepsilon i).$$

La forme admettant ces valeurs pour racines et que nous désignerons par X est

$$\begin{aligned} F_1 = {} & \left[z_1^4 - \frac{\rho^4}{(1+\rho)^4} z_2^4\right]\left[z_1^4 - \frac{\rho^4}{(1-\rho)^4} z_2^4\right] \\ & \times [z_1^2 - \rho^2(1+i)^2 z_2^2][z_1^2 - \rho^2(1-i)^2 z_2^2] \\ = {} & (z_1^8 - 34 z_1^4 z_2^4 + z_2^8)(z_1^4 + z_2^4) \\ = {} & z_1^{12} - 33 z_1^8 z_2^4 - 33 z_1^4 z_2^8 + z_1^{12} = \chi. \end{aligned}$$

En résumé, on obtient

$$\begin{aligned} F_1 &= \chi = z_1^{12} - 33 z_1^8 z_2^4 - 33 z_1^4 z_2^8 + z_2^{12}, \\ F_2 &= W = z_1^8 + 14 z_1^4 z_2^4 + z_2^8, \\ F_3 &= t = z_1 z_2 (z_1^4 - z_2^4). \end{aligned}$$

La fonction W est le hessien de t, et la fonction X est le jacobien de t, W. En effet

$$H(t) = \begin{vmatrix} 20 z_1^3 z_2 & 5(z_1^4 - z_2^4) \\ 5(z_1^4 - z_2^4) & -20 z_1 z_2^3 \end{vmatrix} = -25\,W,$$

$$J(t, W) = \begin{vmatrix} 5 z_1^4 z_2 - z_2^5 & z_1^5 - 5 z_1 z_2^4 \\ 8 z_1^7 + 56 z_1^3 z_2^4 & 56 z_1^4 z_2^3 + 8 z_2^7 \end{vmatrix} = -8\chi.$$

Or, on sait (et l'on démontre d'ailleurs facilement) que si une forme est invariante par rapport à une substitution, et que la

substitution a pour effet de multiplier cette forme par λ, son hessien qui est aussi une forme invariante est multiplié en même temps par λ^2; si, dans les mêmes conditions, deux formes invariantes sont multipliées, l'une par λ, l'autre par μ, leur jacobien est multiplié par $\lambda\mu$. Il suffira donc d'examiner comment varie la fonction t par les substitutions du groupe octaédrique pour connaître en même temps ce que deviennent les fonctions W et X.

Les substitutions du groupe octaédrique comprennent celles du groupe tétraédrique et leurs produits par la substitution

$$(1)\qquad z'_1 = \frac{1+i}{\sqrt{2}} z_1, \qquad z'_2 = \frac{1-i}{\sqrt{2}} z_1.$$

On a vu que les substitutions du groupe tétraédrique laissent t inaltérée; quant aux substitutions (1), elles nous donnent

$$z'^4_1 = -z^4_1, \qquad z'^4_2 = -z^4_2, \qquad z'_1 z'_2 = z_1 z_2,$$

d'où

$$t' = -t.$$

Donc par l'application des substitutions tétraédriques

$$W' = W, \qquad \chi' = \chi$$

et par les substitutions (1)

$$W' = W, \qquad \chi' = -\chi.$$

On a, par suite, dans tous les cas,

$$t'^4 = t^4, \qquad W'^3 = W^3, \qquad \chi'^2 = \chi^2,$$

et le type général des formes fondamentales pour le groupe octaédrique est

$$F = \lambda_1 \chi^2 + \lambda_2 W^3 + \lambda_3 t^4.$$

Pour déterminer les coefficients μ_i de la relation

$$\mu_1 \chi^2 + \mu_2 W^3 + \mu_3 t^4 = 0,$$

il suffira de faire d'abord $z_1 = 1$, $z_2 = 0$; d'où

$$\chi^2 = 1, \qquad W^3 = 1, \qquad t^4 = 0$$

et

$$\mu_1 + \mu_2 = 0,$$

puis de faire $z_1^4 = 1$, $z_2^4 = -1$, d'où

$$\chi^2 = 0, \qquad W^3 = (-12)^3, \qquad t^4 = -2^4$$

et

$$(-12)^3 \mu_2 - 2^4 \mu_3 = 0.$$

On tire de là

$$\mu_1 : \mu_2 : \mu_3 = 1 : -1 : 108.$$

La relation cherchée est donc

$$\chi^2 - W^3 + 108\, t^4 = 0.$$

127. Les nœuds du réseau icosaédrique sont les milieux des 30 arêtes, les centres des 20 faces et les 12 sommets. Nous calculerons directement la forme admettant pour racines les 12 sommets. Pour obtenir les deux autres formes, nous emploierons un raisonnement s'appliquant également au tétraèdre et à l'octaèdre, mais que nous n'avons pas voulu utiliser avant de donner un exemple de calcul direct.

Soit F_3 la forme admettant pour racines les sommets d'un polyèdre régulier à faces triangulaires (tétraèdre, octaèdre ou icosaèdre). Le degré de cette forme est égal au nombre S des sommets du polyèdre. Son hessien $H(F_3)$ sera par suite de degré $2S-4$; le jacobien de F_3 et de $H(F_3)$, soit $J[F_3, H(F_3)]$, sera de degré

$$S + (2S - 4) - 2 = 3S - 6.$$

Or ces formes sont des covariants, c'est-à-dire qu'elles restent invariables ou sont multipliées par un facteur constant lorsqu'on leur applique les substitutions linéaires pour lesquelles F est invariante, ces formes ont donc pour racines des systèmes de points homologues.

D'autre part, d'après les formules du n° 52,

$$S = \frac{n+12}{6},$$

$$F = 2S - 4 = \frac{n}{3} < n,$$

$$A = 3S - 6 = \frac{n}{2} < n;$$

donc

$$H(F_3), \qquad J[F_3, H(F_3)]$$

sont des formes simples et ont respectivement le même degré que les formes cherchées F_2, F_1. On a donc, à un facteur constant près

$$H(F_3) = F_2, \qquad J[F_3, H(F_3)] = F_1.$$

Cela posé, arrivons au calcul de F_3.

Les sommets 1 et 12 ont pour coordonnées $(0, 0, \pm 1)$; les valeurs correspondantes de z sont $z = 0$, $z = \infty$.

Le sommet 2 a pour coordonnées $(\sin l, 0, \cos l)$, ou bien (n° 65) $\left(\frac{2}{r}, 0, \frac{1}{r}\right)$ $(r = \sqrt{5})$. La valeur correspondante de z est [n° 60, formule (2)]

$$z = \frac{2}{r - 1} = \frac{r + 1}{2}.$$

Le sommet 7 a pour coordonnées $(-\sin l, 0, -\cos l)$, ou bien $\left(-\frac{2}{r}, 0, -\frac{1}{r}\right)$; la valeur correspondante de z est

$$z = -\frac{2}{r + 1} = -\frac{r - 1}{2}.$$

Les points du plan représentés par les sommets 3, 4, 5, 6 forment avec le point représenté par le sommet 2 un pentagone régulier ayant pour centre l'origine; les points 8, 9, 10, 11 et le point 7 présentent la même disposition.

La forme cherchée est, par conséquent,

$$\begin{aligned} F_3 &= z_1 z_2 \left[z_1^5 - \left(\frac{r+1}{2}\right)^5 z_2^5\right]\left[z_1^5 + \left(\frac{r-1}{2}\right)^5 z_2^5\right], \\ &= z_1 z_2 (z_1^{10} - 11 z_1^5 z_2^5 - z_2^{10}) \quad (^1). \end{aligned}$$

nous la désignerons par f.

On a

$$\begin{aligned} H(f) &= \begin{vmatrix} 110 z_1^9 z_2 - 330 z_1^4 z_2^6 & 11 z_1^{10} - 396 z_1^5 z_2^5 - 11 z_2^{10} \\ 11 z_1^{10} - 396 z_1^5 z_2^5 - 11 z_2^{10} & -330 z_1^6 z_2^4 - 110 z_1 z_2^9 \end{vmatrix} \\ &= 121(-z_1^{20} - 228 z_1^{15} z_2^5 - 494 z_1^{10} z_2^{10} + 228 z_1^5 z_2^{15} - z_2^{20}), \end{aligned}$$

$$\begin{aligned} &J[f, H(f)] \\ &= 121 \begin{vmatrix} 11 z_1^{10} z_2 - 66 z_1^5 z_2^6 - z_2^{11} & -20 z_1^{19} - 3420 z_1^{14} z_2^5 - 4940 z_1^9 z_2^{10} + 1140 z_1^4 z_2^{15} \\ z_1^{11} - 66 z_1^6 z_2^5 - 11 z_1 z_2^{10} & -1140 z_1^{15} z_2^4 - 4940 z_1^{10} z_2^9 + 3420 z_1^5 z_2^{14} - 20 z_2^{19} \end{vmatrix} \\ &= 2420(z_1^{30} - 522 z_1^{25} z_2^5 - 10\,005 z_1^{20} z_2^{10} - 10\,005 z_1^{10} z_2^{20} + 522 z_1^5 z_2^{25} + z_2^{30}). \end{aligned}$$

---

(1) On passe de cette forme à la forme de M. Klein par le changement de variable (*cf.* note p. 90)

$$z'_1 = z_1, \qquad z'_2 = -z_2.$$

Nous désignerons par H et T les expressions entre parenthèses, d'où

$$f = z_1 z_2 (z_1^{10} - 11 z_1^5 z_2^5 - z_2^{10}),$$
$$H = - z_1^{20} - 228 z_1^{15} z_2^5 - 494 z_1^{10} z_2^{10} + 228 z_1^5 z_2^{15} - z_2^{20},$$
$$T = z_1^{30} - 522 z_1^{25} z_2^5 - 10\,005 z_1^{20} z_2^{10} - 10\,005 z_1^{10} z_2^{20} + 522 z_1^5 z_2^{25} + z_2^{30}.$$

Le groupe icosaédrique est engendrée par les substitutions S, T, U liées entre elles par la relation

$$(1) \qquad S^2 T S^3 T S^2 T = U.$$

Les substitutions S et U ont respectivement pour expression

$$z'_1 = \varepsilon^3 z, \qquad z'_2 = \varepsilon^2 z_2,$$
$$z'_1 = z_2, \qquad z'_2 = - z_1.$$

Il est facile de vérifier que f est invariable par ces deux substitutions. La substitution T étant d'ordre 2, ou bien laisse f invariable, ou bien le multiplie par -1. Ce dernier cas ne peut se présenter, car, autrement, en vertu de (1), U multiplierait f par -1, ce qui n'est pas. Donc T laisse également f invariable. On en conclut que la fonction f, et par suite aussi H et T, est invariable par toutes les substitutions du groupe icosaédrique, et que le type le plus général des formes fondamentales pour le groupe icosaédrique est

$$F = \lambda_1 T^2 + \lambda_2 H^3 + \lambda_3 f^5.$$

Pour déterminer les coefficients de la relation

$$\mu_1 T^2 + \mu_2 H^3 + \mu_3 f^5 = 0,$$

faisons d'abord $z_1 = 1$, $z_2 = 0$, ensuite $z_1 = z_2 = 1$; nous obtenons successivement

$$T = 1, \qquad H = -1, \qquad f = 0,$$
$$T = -20\,008, \qquad H = -496, \qquad f = -11$$

et, par suite,

$$\mu_1 - \mu_2 = 0,$$
$$(-20\,008)^2 \mu_1 + (-496)^3 \mu_2 + (-11)^5 \mu_3 = 0,$$

d'où l'on tire

$$\mu_1 : \mu_2 : \mu_3 = 11^5 : 11^5 : 20\,008^2 - 496^3,$$

ou bien

$$\mu_1 : \mu_2 : \mu_3 = 1 : 1 : 1728.$$

La relation cherchée est donc

$$T^2 + H^3 + 1728 f^5 = 0.$$

128. Les formes ainsi obtenues permettent de construire, dans tous les cas possibles, une fonction représentée par le quotient de deux formes invariantes de même degré, et qui reste invariable quand on lui applique les substitutions du groupe homogène correspondant. Une telle fonction, homogène et de degré zéro en z_1, z_2, est une fonction de z, invariable pour les substitutions du groupe non homogène relatif au polyèdre considéré.

Nous appellerons *fonctions polyédriques*, les fonctions rationnelles de z, qui restent invariables pour toutes les substitutions d'un groupe polyédrique.

Une fonction polyédrique prend la même valeur en un ou plusieurs systèmes de points homologues; si elle ne prend la même valeur qu'en un seul système de points homologues, elle est dite *fondamentale*.

Il est évident que le *degré* [1] *d'une fonction fondamentale est égal à l'ordre du groupe correspondant; et que, réciproquement, si le degré d'une fonction polyédrique est égal à l'ordre du groupe, cette fonction est fondamentale.*

Donc $V(z)$ *désignant une fonction fondamentale, appartenant à un certain groupe, le type général des fonctions fondamentales relatives au même groupe est*

$$\frac{a V(z) + b}{c V(z) + d},$$

a, b, c, d *étant des constantes*. De plus *une fonction fondamentale est tout à fait déterminée, quand on connaît les valeurs qu'elle prend en trois points du plan.*

Nous désignerons par $Z(z)$ la fonction polyédrique fondamentale prenant les valeurs 1, 0, ∞ respectivement aux milieux des

---

(1) On entend par *degré* d'une fonction rationnelle le plus grand des degrés de ses deux termes, la fonction étant supposée réduite à sa plus simple expression.

arêtes, aux centres des faces et aux sommets du polygone sphérique considéré. Bien entendu, nous laissons de côté les groupes cycliques; pour ces groupes on peut prendre

$$Z = \frac{F_1^{\nu_1}}{F_2^{\nu_2}} = \frac{z_1^n}{z_2^n} = z^n.$$

Revenons aux groupes polyédriques; la fonction Z correspondante étant rationnelle est déterminée à un facteur constant près, quand on connaît ses zéros et ses infinis. Nous poserons donc

$$Z = h\frac{F_2^{\nu_2}}{F_3^{\nu_3}}, \qquad Z - 1 = k\frac{F_1^{\nu_1}}{F_3^{\nu_3}},$$

h, k étant deux constantes. La relation (n° 123)

$$\mu_1 F_1^{\nu_1} + \mu_2 F_2^{\nu_2} + \mu_3 F_3^{\nu_3} = 0$$

devient alors

$$\frac{\mu_1}{k}(Z - 1) + \frac{\mu_2}{h} Z + \mu_3 = 0,$$

et comme elle se réduit à une identité, on doit avoir

$$\frac{\mu_1}{k} + \frac{\mu_2}{h} = 0, \qquad -\frac{\mu_1}{k} + \mu_3 = 0,$$

d'où

$$h = -\frac{\mu_2}{\mu_1}, \qquad k = \frac{\mu_1}{\mu_3}$$

et

$$Z = -\frac{\mu_2}{\mu_3}\frac{F_2^{\nu_2}}{F_3^{\nu_3}}, \qquad Z - 1 = \frac{\mu_1}{\mu_3}\frac{F_1^{\nu_1}}{F_3^{\nu_3}},$$

ou bien

$$Z - 1 : Z : 1 = \mu_1 F_1^{\nu_1} : -\mu_2 F_2^{\nu_2} : \mu_3 F_3^{\nu_3},$$

ce qui donne, respectivement, pour les groupes cyclique, diédrique, tétraédrique, octaédrique et icosaédrique,

$$Z = z^n,$$

$$Z = \frac{(z^m + 1)^2}{4z^m},$$

$$Z = \frac{\varphi^3}{\psi^3} = \left(\frac{z^4 + 2i\sqrt{3}\,z^2 + 1}{z^4 - 2i\sqrt{3}\,z^2 + 1}\right)^3,$$

$$Z = \frac{W^3}{108\,t^4} = \frac{(z^8 + 14z^4 + 1)^3}{108\,z^4(z^4 - 1)^4},$$

$$Z = -\frac{H^3}{1728\,f^5} = -\frac{(-z^{20} - 228z^{15} - 494z^{10} + 228z^5 - 1)^3}{1728\,z^5(z^{10} - 11z^5 - 1)^5}.$$

D'après un théorème d'Euler, le nombre des arêtes augmenté de 2 est égal à la somme du nombre des faces et du nombre des sommets. Comme ces trois nombres sont précisément les degrés de F_1, F_2, F_3, on voit que la forme

$$X(z_1, z_2) = \frac{F_2 F_3}{F_1}$$

est de degré 2 et par suite, en appliquant un théorème connu sur les fonctions homogènes,

$$X(z_1, z_2) = z_2^2 X(z, 1).$$

Donc

$$X(z, 1) = \frac{F_2(z, 1) F_3(z, 1)}{F_1(z, 1)}$$

est une fonction rationnelle de z. Si l'on écrit simplement X au lieu de $X(z_1, z_2)$, on aura

$$(1) \qquad z_1 = \frac{\sqrt{X}}{\sqrt{X(z, 1)}}, \qquad z_2 = \frac{z\sqrt{X}}{\sqrt{X(z, 1)}}.$$

D'autre part, en désignant par c la constante $-\frac{\mu_2}{\mu_3}$,

$$Z = c\frac{F_2^{\nu_2}}{F_3^{\nu_1}},$$

et comme le second membre est une fonction homogène de degré zéro en z_1, z_2

$$Z = c\frac{[F_2(z, 1)]^{\nu_2}}{[F_3(z, 1)]^{\nu_3}}.$$

Désignons par $F(z)$ le second membre, F est une fonction rationnelle de z, et l'équation

$$Z = F(z)$$

définit z comme fonction algébrique de z, de même que les équations (1) définissent z_1, z_2 comme fonctions algébrique de Z, X.

129. Un problème analogue au précédent se pose pour le groupe modulaire. Il s'agit de construire une fonction transcendante uniforme de z, possédant la propriété de prendre la même

valeur en des points homologues du réseau modulaire, et en ces points seulement, et de prendre les valeurs 1, 0, ∞ aux nœuds de première, deuxième et troisième espèce. Une telle fonction sera dite *fonction modulaire principale*, tandis que nous appellerons plus généralement *fonction modulaire* toute fonction qui prend toujours la même valeur en des points homologues d'un sous-groupe de Γ [1] et seulement en ces points.

La résolution de ce problème nous sera donnée par la théorie des fonctions elliptiques.

On sait [2] qu'étant donné un couple de périodes primitives $2z_1$, $2z_2$ de la fonction elliptique pu, celle-ci est complètement déterminée. On a, en effet,

$$pu = \frac{1}{u^2} + \sum_s \left[\frac{1}{(u-s)^2} - \frac{1}{u^2}\right],$$

où s prend toutes les valeurs $2mz_1 + 2nz_2$, m et n étant deux entiers positifs ou négatifs qui ne sont pas nuls en même temps. Les *invariants* g_2, g_3 de la fonction elliptique ont des valeurs bien déterminées

$$(1) \qquad g_2 = 60 \sum_s \frac{1}{s^4}, \qquad g_3 = 140 \sum_s \frac{1}{s^6}.$$

A l'aide de ces invariants, on forme le *discriminant* Δ et *l'invariant absolu* J,

$$\Delta = g_2^3 - 27 g_3^2, \qquad J = \frac{g_2^3}{\Delta}.$$

J est une fonction homogène, de degré zéro en z_1, z_2; c'est par suite une fonction du seul rapport $\frac{z_2}{z_1} = z$.

---

(1) Les fonctions analogues pour les groupes polyédriques ne présentent aucun intérêt spécial, puisque les sous-groupes des groupes polyédriques sont des groupes cycliques ou polyédriques.

(2) Pour cette formule et toutes celles qui concernent les fonctions elliptiques, *voir* par exemple Weierstrass-Schwarz, *Formeln und Lehrsätze zum Gebrauche der elliptischen Funktionen,* Göttingen, 1883.

Voici d'autres expressions de g_2, g_3, Δ :

$$g_2 = \left(\frac{\pi}{z_2}\right)^4 \left[\frac{1}{12} + 20\sum_{h=1}^{\infty} \frac{h^3\tau^h}{1-\tau^h}\right],$$

$$g_3 = \left(\frac{\pi}{z_2}\right)^6 \left[\frac{1}{216} - \frac{7}{3}\sum_{h=1}^{\infty} \frac{h^5\tau^h}{1-\tau^h}\right],$$

$$\Delta = \left(\frac{\pi}{z_2}\right)^{12} \tau \prod_{h=1}^{\infty} (1-\tau^h)^{24},$$

où

$$\tau = e^{2\pi i \frac{z_1}{z_2}}.$$

Enfin Δ est, à un facteur constant près, le déterminant fonctionnel de g_2, g_3.

Des relations précédentes résulte

$$J - 1 : J : 1 = 27 g_3^2 : g_2^3 : \Delta.$$

D'après un théorème célèbre de Jacobi, le rapport $\frac{z_1}{z_2}$ ne peut être réel. Comme les parties imaginaires de $\frac{z_1}{z_2}$ et $\frac{z_2}{z_1}$ sont de signes contraires, on peut admettre, sans nuire à la généralité, que la partie imaginaire de $\frac{z_1}{z_2}$ est positive.

Or, on sait qu'une fonction elliptique admet une infinité de couples de périodes primitives et que si $2z_1$, $2z_2$ désigne un tel couple, tout autre couple $2z'_1$, $2z'_2$ est donné par des relations de la forme

$$2z'_1 = \alpha.2z_1 + \beta.2z_2,$$

$$2z'_2 = \gamma.2z_1 + \gamma.2z_2;$$

avec

$$\alpha\delta - \beta\gamma = \pm 1.$$

Si, de plus, pour le nouveau couple, la partie imaginaire de $\frac{z'_1}{z'_2}$ est positive, on aura

$$\alpha\delta - \beta\gamma = + 1.$$

On peut donc dire que si z_1, z_2 est un couple de demi-périodes primitives d'une fonction elliptique, tous les autres couples ana-

logues relatifs à la même fonction s'obtiennent en appliquant au couple z_1, z_2 les substitutions du groupe modulaire homogène. Il en résulte que les fonctions g_2, g_3 et par suite Δ, J restent invariables, si on leur applique les substitutions de ce groupe. Et comme ce sont des fonctions homogènes de z_1, z_2 (de degrés -4, -6, -12, 0), nous les appellerons *formes modulaires absolument invariantes;* ou plus simplement *formes modulaires.* En particulier J est une fonction de z, qui ne change pas quand on lui applique les substitutions du groupe modulaire non homogène; c'est donc une *fonction modulaire principale.*

On sait que g_2, g_3, Δ s'annulent respectivement pour $z = -\frac{1+i\sqrt{3}}{2}$, i, ∞. Donc *la fonction* J *prend, aux nœuds de première, deuxième et troisième espèce du réseau modulaire, respectivement les valeurs* 1, 0, ∞.

De plus, comme les relations (1) peuvent s'écrire

$$z_2^4 g_2 = 60 \sum_{m,n} \frac{1}{(2mz+2n)^4},$$

$$z_2^6 g_3 = 140 \sum_{m,n} \frac{1}{(2mz+2n)^6},$$

on voit que pour des points z, symétriques par rapport à l'axe imaginaire, $z_2^4 g_2$, $z_2^6 g_3$ prennent chacune des valeurs conjuguées [1].

J est donc une fonction modulaire, dont la valeur se transforme

---

[1] Considérons, en effet, la somme $\sum_{m,n} \frac{1}{(mz+n)^4}$; remplaçons z successivement par $x+iy$ et $x-iy$, nous aurons

$$\sum_{m,n} \frac{1}{(mx+n+miy)^4}, \qquad \sum_{m,n} \frac{1}{(-mx+n+miy)^4},$$

ou encore

$$\sum_{m,n} \frac{1}{(mx+n+miy)^4}, \qquad \sum_{m,n} \frac{1}{(mx-n-miy)^4}.$$

Mais puisque n prend toutes les valeurs positives et négatives, nous pourrons, dans la seconde somme, écrire $-n$ au lieu de n. Elle devient alors $\sum_{m,n} \frac{1}{(mx+n-miy)^4}$ et l'on voit qu'elle est conjuguée de la première. On ferait une démonstration analogue pour g_3.

en la valeur conjuguée par la pseudo-substitution $\overline{z'} = -z$. On déduit de là que J *est réelle sur tous les côtés du réseau modulaire.*

130. Soit un réseau régulier représentant un groupe de substitutions linéaires; considérons plus généralement une fonction $Z(z)$, qui, prenant la même valeur aux points homologues de ce réseau, prenne des valeurs conjuguées en des points symétriques par rapport à un quelconque des cercles du réseau et les valeurs 1, 0, ∞ aux nœuds de première, deuxième et troisième espèces. Elle sera réelle sur les côtés de tous les triangles, et, en désignant pour un instant par a, b, c les sommes de première, deuxième et troisième espèce d'un triangle quelconque, cette fonction variera sur le côté ab de 1 à 0, sur le côté bc de 0 à $-\infty$, et sur le côté ac de 1 à ∞. De plus, dans un même triangle la partie imaginaire de $Z(z)$ aura constamment le même signe, et dans deux triangles conjugués des signes contraires : elle aura, par exemple, le signe *plus* dans tous les triangles blancs, et le signe *moins* dans tous les triangles ombrés. Si l'on représente sur un plan les valeurs de la fonction Z, aux points a, b, c du plan z correspondront dans le plan Z les points 1, 0, ∞, et aux côtés ab, bc, ac les segments $1\ldots 0$, $0\ldots-\infty$, $1\ldots+\infty$ de l'axe réel; de plus, à un triangle blanc correspondra tout le demi-plan supérieur, et à un triangle ombré tout le demi-plan inférieur. On voit que dans chaque bitriangle la fonction prend toutes les valeurs possibles. Au réseau tout entier correspond sur le plan Z une *surface de* Riemann dont les feuillets sont en nombre n ou en nombre infini, suivant que le groupe est d'ordre fini n ou d'ordre infini. La correspondance entre les deux plans est *conforme* et cela en vertu des principes généraux de la théorie des fonctions. Il y a exception toutefois aux points de ramification 1, 0, ∞ de la surface de Riemann, pour lesquels nous trouvons des angles π correspondant aux angles $\frac{\pi}{\nu_1}$, $\frac{\pi}{\nu_2}$, $\frac{\pi}{\nu_3}$ du plan z. Il suit de là que z_0 étant un point distinct des nœuds du réseau, et Z_0 la valeur correspondante de Z, on a, k étant une constante différente de zéro,

$$(1) \qquad z - z_0 \equiv k(Z - z_0).$$

Cette notation exprime que $z - z_0$ est égal à $k(z - z_0)$ aux infiniment petits près d'ordre supérieur.

Au contraire, pour les points a, b, c, on aura

$$(2) \qquad z - a = k(\mathrm{Z} - 1)^{\frac{1}{\nu_1}},$$

$$(3) \qquad z - b = k\mathrm{Z}^{\frac{1}{\nu_2}},$$

$$(4) \qquad z - c = k\mathrm{Z}^{-\frac{1}{\nu_3}}.$$

Ces formules ne sont pas applicables si $\nu_i = \infty$, c'est-à-dire si l'un des angles du réseau est nul. Supposons, par exemple, $\nu_2 = \infty$; on remplacera la formule (3) par la suivante :

$$(5) \qquad z - b = \frac{k}{\operatorname{Log} \mathrm{Z} + l} \quad (^1).$$

Nous représenterons par la notation $z(\nu_1, \nu_2, \nu_3; \mathrm{Z})$ la fonction z considérée comme fonction de Z.

131. De là résulte un théorème important.

Étant données les deux fonctions $z(\nu_1, \nu_2, \nu_3; \mathrm{Z})$, $z'(\nu'_1, \nu'_2, \nu'_3; \mathrm{Z})$ où ν_1, ν_2, ν_3 sont respectivement multiples de ν'_1, ν'_2, ν'_3. Si $\nu_i = \infty$, nous le considérerons comme multiple de ν'_i, que ν'_i soit fini ou non. Il existera pour z' des relations analogues aux relations (1),

---

(1) Voici comment on peut parvenir à cette formule :

Si $\nu_2 = \infty$, le point b est sur l'axe réel et les deux côtés du triangle passant par b ont leur tangente commune parallèle à l'axe imaginaire. Soient en grandeur et en signe α, β les rayons des cercles auxquels appartiennent ces côtés ; ces cercles auront pour équation

$$(x - b)^2 + y^2 - 2\alpha(x - b) = 0, \qquad (x - b)^2 + y^2 - 2\beta(x - b) = 0.$$

Par la substitution $z' = -\frac{1}{z - b}$, les cercles se changent en deux droites parallèles à l'axe y', ayant pour équations

$$x' = -\frac{1}{2\alpha}, \qquad x' = -\frac{1}{2\beta}.$$

On sait qu'un faisceau de droites parallèles se change en un faisceau de droites concourantes par une transformation de la forme

$$z' = e^{\mu z + \nu}.$$

Dans le cas actuel, nous poserons

$$z = e^{i(pz' + q)},$$

(2), (3), (4), (5) du paragraphe précédent. On a

$$z' - z'_0 \equiv \frac{k'}{k}(z - z_0),$$

$$z' - a' \equiv \frac{k'}{k^{\frac{\nu_1}{\nu'_1}}}(z - a)^{\frac{\nu_1}{\nu'_1}},$$

$$z' - b' \equiv \frac{k'}{k^{\frac{\nu_2}{\nu'_2}}}(z - b)^{\frac{\nu_2}{\nu}},$$

$$z' - c' \equiv \frac{k'}{k^{\frac{\nu_3}{\nu'_3}}}(z - c)^{\frac{\nu_3}{\nu'_3}}.$$

Si $\nu_2 = \infty$, ν'_2 étant fini, on obtient

$$z' - b' \equiv k' e^{-\frac{1}{\nu'_2}} e^{\frac{k}{\nu'_2 (z-b)}}.$$

Si $\nu_2 = \infty$, $\nu'_2 = \infty$, on obtient au contraire

$$z' - b' \equiv \frac{k'(z - b)}{(l' - l)(z - b) + k}.$$

---

p et q étant des constantes réelles. En effet, si $Z = Re^{i\Theta}$, nous aurons

$$R = e^{-py'}, \qquad \Theta = px' + q,$$

en sorte que, aux droites $x' =$ const. correspondront les droites $\Theta =$ const., et en particulier aux deux droites considérées les droites

$$\Theta = -\frac{p}{2\alpha} + q, \qquad \Theta = -\frac{p}{2\beta} + q.$$

Si enfin nous voulons que ces deux rayons soient les deux moitiés de l'axe des x, on devra avoir

$$0 = -\frac{p}{2\alpha} + q, \qquad \pi = -\frac{p}{2\beta} + q,$$

d'où

$$p = \frac{2\pi\alpha\beta}{\beta - \alpha}, \qquad q = \frac{\pi\beta}{\beta - \alpha},$$

on a donc

$$Z = e^{i\left(-\frac{p}{z-b} + q\right)},$$

d'où

$$z - b = \frac{-ip}{\log Z - iq}.$$

Ces formules montrent que : *Si les* ν_i *sont respectivement multiples des* ν'_i, z' *est une fonction uniforme de* z.

Donnons de suite quelques applications de ce théorème.

a. Les réseaux du groupe diédrique pour $m = 3$ et des groupes tétraédrique, octaédrique et icosaédrique ont respectivement pour symboles

$$(2, 3, 2), \quad (2, 3, 3), \quad (2, 3, 4), \quad (2, 3, 5);$$

tandis que le réseau modulaire a pour symbole $(2, 3, \infty)$. Donc :

Si les variables Z, z, z' *sont liées par les deux relations*

$$Z = F(z'), \qquad Z = J(z),$$

F *désignant l'une des quatre fonctions*

$$\frac{(z^3+1)^2}{4z^3}; \quad \frac{\varphi^3}{\psi^3}, \quad \frac{W^3}{108\,t^4}, \quad -\frac{H^3}{1728 f^5},$$

et J *étant la fonction définie au n°* 129, z' *est une fonction uniforme de* z.

b. Le triangle fondamental du sous-groupe Γ_6 de Γ a ses trois angles nuls. Si $\lambda(z)$ représente une fonction ayant pour champ fondamental un couple de triangles du réseau Γ_6, z considéré comme fonction de λ pourra s'écrire $z(\infty, \infty, \infty; \lambda)$.

D'où il suit que, quelle que soit la fonction $z'(\nu'_1, \nu'_2, \nu'_3; \lambda)$, z' sera une fonction uniforme de z.

Existence des fonctions modulaires.

132. Nous avons désigné sous le nom de *fonction modulaire* toute fonction invariante dans un sous-groupe du groupe modulaire.

Cherchons maintenant si à chaque sous-groupe de Γ correspondent des fonctions modulaires.

Nous démontrerons qu'il en est bien ainsi pour tout sous-groupe Γ_s de Γ, d'indice finie s.

La relation

$$J = J(z)$$

établit une représentation *conforme* du plan de la variable J sur

un bitriangle du réseau modulaire. Puisque J prend des valeurs réelles sur les côtés du réseau, aux deux moitiés du bitriangle correspondront respectivement les deux moitiés du plan J séparées par l'axe réel. Nous établirons qu'au triangle blanc correspond le demi-plan supérieur, au triangle ombré le demi-plan inférieur.

La représentation cesse d'être conforme aux points 1, 0, ∞ du plan J; en effet au point 1 du plan J par exemple les deux portions de l'axe des x font un angle plat (angle de 180°), tandis que les lignes correspondantes du plan z font un angle de 90°.

Aux bitriangles en nombre infini du réseau modulaire correspondent des feuillets en nombre infini coïncidant avec le plan J; et, si dans le plan z on passe d'un bitriangle à un autre en tournant autour d'un nœud du réseau, on passera en même temps dans le plan J d'un feuillet à un autre en tournant autour d'un des points 1, 0, ∞. L'ensemble des feuillets coïncidant avec le plan J constitue une *surface de* Riemann, à un nombre infini de feuillets, ayant pour points de ramification les points 1, 0, ∞.

Soient donc Γ_s un sous-groupe d'indice fini s, C_s son champ fondamental. A C_s correspondra un ensemble R_s de s feuillets de la surface de Riemann située sur le plan J.

Pour réaliser cette correspondance nous pouvons déformer le bitriangle et l'amener à coïncider avec le plan des J tout entier, de façon que les nœuds tombent aux points 1, 0, ∞.

Entre la surface R_s et la surface fermée à laquelle se ramène le champ C_s (*cf.* n° 83) il existe une correspondance biunivoque; donc, d'après un théorème connu, les deux surfaces sont du même genre.

On peut d'ailleurs le vérifier directement. En effet, on a trouvé pour le genre p de la surface fermée C_s (n° 86)

$$p = 1 - s + \frac{1}{2}\sum_{i=1}^{S}(m_i - 1),$$

$2m_i$ désignant le nombre des arêtes aboutissant à un nœud d'ordre i, et S le nombre des nœuds. D'autre part la théorie des surfaces algébriques nous donne, pour le genre d'une surface de Riemann,

$$p = 1 - s + \frac{1}{2}\sum_{i=1}^{S}(m_i - 1),$$

s étant le nombre des feuillets de la surface, m_i le nombre des feuillets qui se croisent à point de ramification d'ordre i et S le nombre de points de ramification. Or, le nombre des bitriangles de C_s est égal au nombre des feuillets de R_s; à chaque nœud de C_s correspond un point de ramification de R_s ([1]), et à chaque bitriangle ayant pour sommet un nœud de C_s correspond dans R_s un feuillet qui se croise avec d'autres feuillets au point de ramification correspondant. Donc les deux valeurs de p sont égales.

En vertu des théorèmes d'existence de Riemann, il existe des fonctions de J, uniformes sur la surface R_s. Soit y l'une d'elles, y et J sont liés par une relation algébrique

$$f(y, \mathrm{J}) = 0. \tag{1}$$

Puisque y est uniforme sur R_s, et que C_s et R_s se correspondent point par point, on peut dire que y prend une valeur unique en chaque point de C_s. De plus, comme chaque point de R_s correspond à une infinité de points du plan z et correspond par suite à tous les points de Γ_s homologues d'un même point de C_s, on peut dire que y, regardée comme fonction de z, reprend la même valeur aux points homologues dans C_s. En d'autres termes, y est une fonction modulaire relative au sous-groupe Γ_s. Donc :

Étant donné un sous-groupe Γ_s de Γ d'indice fini s, il existe des fonctions modulaires relatives à ce sous-groupe; elles sont liées à J par des relations algébriques.

Toute autre fonction modulaire relative à Γ_s est une fonction uniforme sur R_s et par conséquent une fonction rationnelle de y, J.

Il est facile de voir que les différentes racines de l'équation (1) sont des fonctions modulaires relatives à autant de sous-groupes équivalents à Γ_s et par suite représentés par le réseau C_s. Soient 1, $S_1, S_2, \ldots, S_{s-1}$ les symboles des s bitriangles du réseau modulaire qui constituent le champ C_s; les valeurs de y en s points du

(1) Les seuls points de ramification de R_s sont les points 1, 0, ∞; considérons un de ces points et supposons que les feuillets qui s'y croisent comprennent $h_1, h_2, \ldots, h_r$ feuillets formant chacun un cycle, on considérera le point correspondant comme un ensemble de r points de ramification respectivement d'ordres $h_1 - 1, h_2 - 1, \ldots, h_r - 1$.

champ C_s homologues dans Γ, ou bien en s points superposés de R_s seront

$$(2)\qquad \begin{cases} y(z) = y(z), \quad y_1(z) = y[S_1(z)], \quad \ldots, \\ y_{s-1}(z) = y[S_{s-1}(z)]. \end{cases}$$

Or, P étant une substitution quelconque de Γ_s, on a

$$y[P(z)] = y(z);$$

si dans cette relation on remplace z par $S_i(z)$, on a

$$(3)\qquad y[S_iP(z)] = y[S_i(z)] = y_i(z).$$

D'autre part les relations (2) peuvent s'écrire

$$y_i[S_i^{-1}(z)] = y(z).$$

Remplaçons z par $S_iP(z)$, il vient

$$y_i[S_iPS_i^{-1}(z)] = y[S_iP(z)]$$

et, par suite, à cause de (3),

$$y_i[S_iPS_i^{-1}(z)] = y_i(z).$$

Donc $y_i(z)$ *est une fonction modulaire relative au sous-groupe* $S_i\Gamma_sS_i^{-1}$ *équivalent à* Γ_s.

133. Examinons en particulier le cas où Γ_s est un sous-groupe invariant. Alors toutes les racines de

$$f(y, J) = 0$$

sont des fonctions modulaires appartenant au sous-groupe Γ_s et sont par suite des fonctions rationnelles de l'une d'elles et de J

$$(1)\qquad y_i = \rho_i(y, J) \qquad (i = 1, 2, \ldots, s-1).$$

La relation (1) peut être considérée comme une transformation de R_s en elle-même, dans laquelle le point (y, J) se change en (y_i, J). Il est clair que les transformations (1) auxquelles on adjoindrait l'identité, forment un groupe qui, aux notations près, coïncide avec le groupe G_s des transformations de la surface fermée C_s en elle-même (n° 83).

Voici maintenant les différents cas possibles :

a. Si $p = 0$, on peut faire correspondre R_s point par point à un

plan u; y et J sont exprimables rationnellement à l'aide de u

$$y = E(u), \qquad J = F(u),$$

u étant elle-même une fonction modulaire du sous-groupe considéré ; et l'équation

$$(2) \qquad J = F(u)$$

n'est autre que l'équation (1) du paragraphe précédent (p. 222) sous la forme spéciale qu'elle prend dans le cas considéré. On peut la mettre aussi sous la forme

$$J - 1 : J : 1 = \varphi(u) : \psi(u) : \chi(u),$$

$\varphi(u)$, $\psi(u)$, $\chi(u)$ étant trois fonctions rationnelles liées par la relation

$$\varphi(u) = \psi(u) - \chi(u).$$

Toutes les racines de (2) pouvent s'exprimer rationnellement à l'aide de J et d'une quelconque d'entre elles; mais J étant une fonction rationnelle de u, on peut dire que toutes les racines peuvent s'exprimer rationnellement à l'aide d'une quelconque d'entre elles. Il suit de là que deux racines quelconques sont fonctions linéaires l'une de l'autre; on aura par exemple

$$u_i = \frac{\alpha_i u + \beta_i}{\gamma_i u + \delta_i} \qquad (i = 1, 2, \ldots, s-1).$$

b. Soit en second lieu $p = 1$, la surface R_s est elliptique. Nous pouvons prendre deux fonctions u, v régulières sur R_s, liées par la relation

$$v^2 = \rho(u),$$

$\rho(u)$ étant un polynome du troisième degré; et toutes les fonctions régulières sur R_s s'exprimeront rationnellement en u et v, de sorte que, en posant

$$u[S_i(z)] = u_i(z), \qquad v[S_i(z)] = v_i(z),$$

on aura

$$(3) \qquad u_i = H_i(u, v), \qquad v_i = K_i(u, v),$$

H_i, K_i étant des symboles de fonctions rationnelles. Si l'on considère u, v comme les coordonnées des points d'une cubique, les

équations (3) représentent un groupe de transformations rationnelles de cette courbe en elle-même.

c. Soit maintenant $p > 2$ et supposons que la surface R_s ne soit pas hyperelliptique. Désignons par

$$Q_h(y, J) \qquad (h = 1, 2, \ldots, p)$$

un système de polynomes adjoints d'ordre $n - 3$, linéairement indépendants; il leur correspond un système d'intégrales abéliennes de première espèce linéairement indépendantes

$$I_h = \int \frac{Q_h(y, J)}{\frac{\partial f(y, J)}{\partial y}} dJ \qquad (h = 1, 2, \ldots, p).$$

Si dans I_h, nous remplaçons y par y_i, I_h se change en une autre intégrale

$$I_h^{(i)} = \int \frac{Q_h(y_i, J)}{\frac{\partial f(y_i, J)}{\partial y_i}} dJ.$$

Les valeurs que prend I_h en s points de R_s, où J a une même valeur, coïncident avec celles que prend $I_h^{(i)}$ aux mêmes points; I_h étant toujours fini, il en est de même de $I_h^{(i)}$. $I_h^{(i)}$ est une intégrale de première espèce et $Q_h(y_i, J)$ un polynome adjoint d'ordre $n - 3$, par conséquent une fonction linéaire de $Q_1(y, J)$, $Q_2(y, J)$, ..., $Q_p(y, J)$, d'où

$$(4) \quad \begin{cases} Q_1(y_i, J) = \alpha_{11}^{(i)} Q_1(y, J) + \ldots + \alpha_{ip}^{(i)} Q_p(y, J), \\ Q_2(y_i, J) = \alpha_{21} \; Q_1(y, J) + \ldots + \alpha_{2p} R_p(y, J), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ Q_p(y_i, J) = \alpha_{p1}^{(i)} Q_1(y, J) + \ldots + \alpha_{pp}^{(i)} Q_p(y, J) \\ \qquad (i = 1, 2, \ldots, s - 1). \end{cases}$$

Les $Q_h(y, J)$ $(h = 1, 2, 3, \ldots, p)$ sont p fonctions modulaires linéairement indépendantes du sous-groupe considéré, et les relations (4) représentent la transformation qu'elles subissent quand on passe de y à y_i, c'est-à-dire quand on applique à z la substitution S_i. Donc les transformations (4) constituent, avec l'identité, un groupe holoédriquement isomorphe au groupe G_s.

Le groupe des transformations (4) est susceptible d'une interprétation géométrique remarquable.

On sait qu'on appelle *courbe normale de* Noether la courbe de l'espace à $p-1$ dimensions dont les points ont pour coordonnées homogènes $Q_1(y, J)$, $Q_2(y, J)$, ..., $Q_p(y, J)$. Or, les relations (4) représentent une collinéation, pour laquelle la courbe normale se transforme en elle-même. Nous pouvons donc dire que le groupe G_s coïncide aux notations près avec le groupe des collinéations qui transforment en elle-même la courbe normale de Noether.

d. Les considérations précédentes ne s'appliquent plus, quand p étant supérieur ou égal à 2, la surface R_s est hyperelliptique (ce qui a lieu nécessairement si $p=2$).

Dans ce cas, on peut remplacer R_s par une autre surface de Riemann, R'_2 à deux feuillets et $2p+1$ ou $2p+2$ points de ramification; en d'autre termes, on peut choisir deux fonctions u, v régulières sur R_s, liées par une relation de la forme

$$v^2 = \rho(u),$$

ρ étant un polynome de degré $2p+1$ ou $2p+2$. Alors toute fonction W régulière sur R_s est de la forme

$$w = \frac{\lambda(u) + v\mu(u)}{\nu(u)}, \tag{5}$$

$\lambda(u)$, $\mu(u)$, $\nu(u)$ étant des polynomes en u premiers entre eux.

Désignons par $u(z)$ l'expression u considérée comme fonction de z et posons

$$u[S_i(z)] = u_i(z).$$

Puisque, sur R_s, u prend deux fois la même valeur, il en sera de même pour u_i, en sorte que, en posant d'après (5)

$$u_i = \frac{\lambda(u) + v\mu(u)}{\nu(u)},$$

la fonction

$$\lambda(u) + v\mu(u) - u_i\nu(u) \tag{6}$$

devra pour chaque valeur de u_i s'annuler en deux points de R_s. Mais v prenant une même valeur en $2p+1$ ou $2p+2$ points, c'est-à-dire en plus de deux points, il ne peut y avoir dans (6) de terme en v et, d'après la nature de u, $\lambda(u)$ et $\nu(u)$ devront

être linéaires. On en conclut que u_i est liée à u par une relation linéaire de la forme

$$(7) \qquad u_i = \frac{\alpha_i u + \beta i}{\gamma_i u + \delta i}.$$

Recherchons maintenant si u, u_1, u_2, ..., u_{s-1} sont ou non toutes distinctes, en d'autres termes si les substitutions linéaires (7) forment, avec l'identité, un groupe d'ordre égal ou inférieur à s.

Observons que (n° 98), si $p > 1$, on a $n > 6$; par suite, dans le réseau considéré, il y a plus de 6 bitriangles se croisant en un nœud de troisième espèce, et l'opération S considérée comme appartenant à G_s est d'ordre supérieur à 6.

Or les seuls groupes finis de substitutions contenant des opérations d'ordre supérieur à 6 sont certains groupes cycliques et diédriques; d'autre part, les seuls groupes cycliques et diédriques appartenant au type G_s correspondent aux symboles (2, 1, 2), (2, 3, 2), (1, 3, 3) (n° 98) et ne contiennent pas de substitutions d'ordre 6. Donc le groupe formé par les substitutions (7), ne saurait coïncider avec G_s et par conséquent les u, u_1, ..., u_{s-1} ne sont pas toutes distinctes.

Il existe donc une transformation non identique de C_s en lui-même, à laquelle correspond la transformation de u en elle-même, c'est-à-dire un échange de deux feuillets de R'_2; et il est bien clair que c'est la seule transformation de cette espèce. Donc l'ordre du groupe (7) est $\frac{s}{2}$. En combinant ce groupe $G_{\frac{s}{2}}$ avec la substitution $v' = -v$, on obtient le groupe G_s.

Le groupe $G_{\frac{s}{2}}$ est de genre zéro, parce que, en prenant une seule fois chacune de ses valeurs sur la surface de Riemann correspondante, cette surface peut se réduire à un plan unique.

Le polygone générateur de $\Gamma_{\frac{s}{2}}$ est l'ensemble des bitriangles de C_s, qui, dans la transformation de C_s en R_s et ensuite en R'_2, donnent lieu à un feuillet de R'_2. Le sous-groupe $\Gamma_{\frac{s}{2}}$ est invariant, parce que les u_i, étant des fonctions rationnelles de u, appartiennent toutes au même groupe.

Comme le nombre de bitriangles se croisant sur la surface S en

un nœud de troisième espèce, est supérieur à 6, pour la surface $C_{\frac{s}{2}}$, on aura $n > 3$, c'est-à-dire $n = 4$ ou $n = 5$, et par suite $\frac{s}{2} = 24$, $\frac{s}{2} = 60$.

Ainsi donc, quand la surface R_s est hyperelliptique, les seuls cas possibles sont

$$\begin{aligned} s &= 48, \quad 120, \\ n &= \ 8, \quad 10. \end{aligned}$$

La formule (2) (n° 98)

$$s = \frac{12r(p-1)}{r-6},$$

où l'on doit remplacer r par n, donne ensuite dans les deux cas

$$p = 2 \quad \text{et} \quad p = 5.$$

Construction des formes modulaires.

134. Nous venons d'établir l'existence des fonctions modulaires pour n'importe quel sous-groupe.

Occupons-nous maintenant de leur construction effective dans quelques cas simples.

D'après la théorie des fonctions elliptiques, on sait que, si $2z_1$, $2z_2$ et $2z'_1$, $2z'_2$ sont deux couples de périodes primitives, on a

$$(1) \qquad \sigma(u \mid z'_1, z'_2) = \sigma(u \mid z_1, z_2).$$

De plus m_1, m_2 désignant deux nombres entiers quelconques

$$(2) \quad \sigma(u + 2m_1z_1 + 2m_2z_2) = (-1)^{m_1m_2+m_1+m_2} e^{2(m_1\eta_1+m_2\eta_2)(u+m_1z_1+m_2z_2)}\sigma u,$$

avec

$$\eta_i = \zeta z_i \qquad (i = 1, 2).$$

Les z_i et les η_i sont liés par la relation connue

$$(3) \qquad z_1\eta_2 - z_2\eta_1 = \frac{\pi i}{2},$$

moyennant l'hypothèse déjà faite que la partie imaginaire de $\frac{z_1}{z_2} = z$ est positive.

En particulier, n étant un nombre entier, posons

(4) $$z'_1 = z_1 + n z_2, \qquad z'_2 = z_2,$$

et remplaçons dans (1) u par

$$u = \frac{2 z'_1}{n} = \frac{2 z_1}{n} + 2 z_2.$$

Nous aurons, à cause de (2),

(5) $$\sigma\left(\frac{2 z'_1}{n} \middle| z'_1, z'_2\right) = \sigma\left(\frac{2 z'_1}{n} \middle| z_1, z_2\right) = \sigma\left(\frac{2 z_1}{n} + 2 z_2 \middle| z_1, z_2\right)$$
$$= e^{2\eta_2\left(\frac{2 z_1}{n} + z_2\right)} \sigma\left(\frac{2 z_1}{n} \middle| z_1, z_2\right).$$

Or, en tenant compte de

$$\eta'_1 = \eta_1 + n \eta_2,$$

on a

$$z'_1 \eta'_1 = (z_1 + n z_2)(\eta_1 + n \eta_2) = z_1 \eta_1 + \eta(z_1 \eta_2 + z_2 \eta_1) + n^2 z_2 \eta_2,$$

et, à cause de (3),

$$z'_1 \eta'_1 = z_1 \eta_1 + 2 n z_1 \eta_2 + n^2 z_2 \eta_2 - \frac{n \pi i}{2},$$

$$2\eta_2\left(\frac{2 z_1}{n} + z_2\right) + \pi i = \frac{2 z'_1 \eta'_1}{n^2} - \frac{2 z_1 \eta_1}{n^2} + \frac{n+1}{n} \pi i;$$

d'où pour (5)

$$e^{-\frac{2 z'_1 \eta'_1}{n^2}} \sigma\left(\frac{2 z'_1}{n} \middle| z'_1, z'_2\right) = e^{\frac{n+1}{n}\pi i} e^{-\frac{2 z_1 \eta_1}{n^2}} \sigma\left(\frac{2 z_1}{n} \middle| z_1, z_2\right).$$

Si n est pair, $e^{\frac{n+2}{n}\pi i} = e^{\frac{n+1}{2n} 2\pi i}$ est une racine d'ordre $2n$ de l'unité ; au contraire si n est impair, en posant $n = 2p + 1$, on a $e^{\frac{n+1}{n}\pi i} = e^{\frac{p+1}{n} 2\pi i}$, qui est une racine d'ordre n de l'unité [1]. On peut donc dire que par la substitution (4) ou encore pour la substitution S^n, la fonction

$$e^{-\frac{2 z_1 \eta_2}{n^2}} \sigma\left(\frac{2 z_1}{n} \middle| z_1, z_2\right)$$

---

[1] La relation $n = 2(p+1) - 1$ montre que n et $p+1$ sont premiers entre eux.

est multipliée par une racine d'ordre $2n$ ou n de l'unité, suivant que n est pair ou impair.

Posons maintenant

$$(6)\quad \sigma_{hk}(u \mid z_1, z_2) = e^{\frac{2h\eta_1+2k\eta_2}{n}\left(u-\frac{hz_1+kz_2}{n}\right)}\sigma\left(u - \frac{2hz_1+2kz_2}{n}\,\middle|\, z_1, z_2\right),$$

$$(7)\quad \sigma_{hk}(0 \mid z_1, z_2) = -e^{-\frac{2(h\eta_1+k\eta_2)(kz_1+kz_2)}{n^2}}\sigma\left(\frac{2hz_1+2kz_2}{n}, z_1, z_2\right) = \sigma_{hk}(z_1, z_2),$$

et appliquons à z_1, z_2 la substitution modulaire homogène

$$(8)\qquad V = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} an+1 & bn \\ cn & dn+1 \end{pmatrix} \equiv 1 \pmod{n},$$

désignons par $\sigma'_{hk}u$ ce que devient $\sigma_{hk}u$, quand on lui applique la substitution (8) et observons que

$$\eta'_1 = \alpha\eta_1 + \beta\eta_2 = (an+1)\eta_1 + bn\eta_2,$$
$$\eta'_2 = \gamma\eta_1 + \delta\eta_2 = cn\eta_1 + (dn+1)\eta_2.$$

Posons pour abréger

$$ha + kc = \mathrm{L}, \qquad hd + kd = \mathrm{M},$$
$$h\eta_1 + k\eta_2 = \eta, \qquad hz_1 + hz_2 = z,$$
$$\mathrm{L}\eta_1 + \mathrm{M}\eta_2 = \mathrm{H}, \qquad \mathrm{L}z_1 + \mathrm{M}z_2 = \mathrm{Z};$$

on tire de (6), en tenant compte de (1),

$$\sigma'_{hk}u = e^{2\left(\mathrm{H}+\frac{\eta}{u}\right)\left(u-\mathrm{Z}-\frac{z}{n}\right)}\sigma\left(u - 2\mathrm{Z} - \frac{2z}{n}\,\middle|\, z_1, z_2\right).$$

Or, d'après (2),

$$\sigma\left(u - 2\mathrm{Z} - \frac{2z}{n}\right) = (-1)^{\mathrm{LM}+\mathrm{L}+\mathrm{M}}e^{-2\mathrm{H}\left(u-\mathrm{Z}-\frac{2z}{n}\right)}\sigma\left(u - \frac{2z}{n}\right),$$

et, d'après (6),

$$\sigma\left(u - \frac{2z}{n}\right) = e^{-\frac{2\eta}{u}\left(u-\frac{z}{n}\right)}\sigma_{hk}u;$$

on a donc, après quelques réductions,

$$\sigma'_{hk}u = (-1)^{\mathrm{LM}+\mathrm{L}+\mathrm{M}}e^{\frac{2}{n}(\mathrm{H}z-\eta\mathrm{Z})}\sigma_{hk}u.$$

De plus

$$\mathrm{LM}+\mathrm{L}+\mathrm{M} = h^2ab + hk(ad+bc) + k^2cd + h(a+b) + k(c+d):$$
$$(-1)^h = (-1)^{h^2}, \qquad (-1)^k = (-1)^{k^2};$$

par suite

$$(-1)^{\mathrm{LM}+\mathrm{L}+\mathrm{M}} = (-1)^{h^2(ab+a+b)+hk(ad+bc)+k^2(cd+c+d)}.$$

D'autre part (3) donne

$$\begin{aligned}\mathrm{H}z - \eta\mathrm{Z} &= (\mathrm{L}\eta_1 + \mathrm{M}\eta_2)(hz_1 + kz_2) - (h\eta_1 + k\eta_2)(\mathrm{L}z_1 + \mathrm{M}z_2)\\ &= (\mathrm{M}h - \mathrm{L}k)(z_1\eta_2 - z_2\eta_1) = (\mathrm{M}h - \mathrm{L}k)\frac{\pi i}{2}\\ &= [h^2 b + hk(d-a) - k^2 c]\frac{\pi i}{2}.\end{aligned}$$

Donc

$$(9)\quad \left\{\begin{aligned}\sigma'_{hk}u &= (-1)^{h^2(ab+a+b)+hk(ad+bc)+k^2(cd+c+d)} \times e^{\frac{\pi i}{n}[h^2 b + hk(d-a) - k^2 c]}\sigma_{hk}u\\ &= e^{\frac{\pi i}{n}[h^2(nab+na+nb+b)+hk(nad+nbc+d-a)+k^2(ncd+nc+nd-c)]}\sigma_{hk}u.\end{aligned}\right.$$

Ainsi, par les substitutions (8), c'est-à-dire par les substitutions du groupe homogène $\Gamma_{2\mu(n)}$, $\sigma_{hk}u$ est multipliée par une racine de l'unité, ce qui montre qu'une certaine puissance de $\sigma_{hk}u$ reste invariable; en d'autres termes, $\sigma^r_{hk}u$ où r est un certain nombre entier est une forme invariante dans le groupe homogène $\Gamma_{2\mu(n)}$.

135. Voyons maintenant quelles sont parmi les substitutions (8) celles qui laissent invariables toutes les fonctions $\sigma_{hk}u$. De la relation

$$1 = \alpha\delta - \beta\gamma = (an+1)(dn+1) - bcn^2 = (ad-bc)n^2 + (a+d)n + 1$$

on déduit

$$(1)\qquad n(ad-bc) + a + d = 0.$$

Distinguons plusieurs cas :

1° Soit n impair. Alors (1) donne

$$ad + bc \equiv ad - bc \equiv -(a+d) \equiv d - a \pmod 2.$$

D'autre part, en écrivant (1) sous la forme

$$d(an+1) + a - bcn = a(dn+1) + d - bcn = 0,$$

on voit que si a ou d est impair, b et c le sont également, en sorte que les produits $a(b+1)$ et $d(c+1)$ sont toujours pairs

$$ab + a \equiv dc + b \equiv 0 \pmod 2.$$

D'après cela la relation (9) du paragraphe précédent (p. 231) peut s'écrire

$$\sigma'_{hk} u = (-1)^{h^2b+hk(d-a)-k^2c} e^{\frac{\pi i}{n}[h^2b+hk(d-a)-k^2c]} \sigma_{hk} u,$$

ou bien

$$(2) \qquad \sigma'_{hk} u = e^{\pi i \frac{n-1}{n}[-h^2b+hk(a-d)+k^2c]} \sigma_{hk} u.$$

Pour que toutes les $\sigma_{hk} u$ restent invariables, il faut et il suffit (en tenant compte de ce que $n-1$ est pair) que la quantité entre crochets soit un multiple de n pour tout système de valeurs de h, k, c'est-à-dire que l'on ait

$$b \equiv c \equiv a - d \equiv 0 \qquad (\operatorname{mod} n).$$

D'autre part, d'après (1),

$$a + d \equiv 0 \qquad (\operatorname{mod} n);$$

d'où

$$a \equiv b \equiv c \equiv d \equiv 0 \qquad (\operatorname{mod} n),$$

et a', b', c', d' étant des nombres entiers,

$$a = a'n, \qquad b = b'n, \qquad c = c'n, \qquad d = d'n;$$

nous avons alors

$$V = \begin{pmatrix} \alpha & \beta \\ \gamma & \gamma \end{pmatrix} = \begin{pmatrix} a'n^2+1 & b'n^2 \\ c'n^2 & d'n^2+1 \end{pmatrix} \equiv 1 \qquad (\operatorname{mod} n^2).$$

Donc : *Pour n impair les substitutions de* Γ (¹)*, laissant invariables toutes les $\sigma_{hk} u$, sont les substitutions du sous-groupe homogène* $\Gamma_{2\mu(n^2)}$.

2° Soit maintenant n pair. Puisque toutes les $\sigma_{hk} u$ restent invariables, la quantité entre crochets figurant au second nombre de la relation (9) (p. 231) est un multiple de $2n$ pour tous les couples de valeurs h, k. On aura donc

$$(3) \qquad \left.\begin{cases} nab + na + nb + b \equiv 0 \\ nad + nbc + d - a \equiv 0 \\ ncd + nc + nd - c \equiv 0 \end{cases}\right\} \qquad (\operatorname{mod} 2n).$$

(¹) Pour plus de précision on devrait dire : du groupe homogène correspondant au groupe non homogène Γ.

Ajoutant à la seconde de ces congruences la congruence

$$-2nbc \equiv 0 \pmod{2n},$$

on obtient

$$n(ad - bc) + d - a \equiv 0 \pmod{2n},$$

ce qui donne avec (1)

$$a \equiv d \equiv 0 \pmod{n}.$$

La première des relations (3) devient alors, l désignant un nombre entier,

$$n^2 l + (n+1)b \equiv 0 \pmod{2n},$$

ou, remarquant que, si n est pair, n^2 est divisible par $2n$,

$$(n+1)b \equiv 0 \pmod{2n},$$

et comme $n+1$ est premier avec n,

$$b \equiv 0 \pmod{2n}.$$

La dernière des relations (3) donne, en opérant d'une façon analogue,

$$c \equiv 0 \pmod{2n}.$$

Nous pouvons par suite écrire, a', b', c', d' étant des entiers,

$$a = a'n, \qquad b = 2b'n, \qquad c = 2c'n, \qquad d = d'n,$$

et transportant ces valeurs dans la seconde des relations (3)

$$n^3(a'd' + 4b'c') + n(d' - a') \equiv 0 \pmod{2n}$$

ou bien

$$d' - a' \equiv 0 \pmod{2}.$$

Posons donc

$$a' = 2a'' + \varepsilon,$$

où ε est égal à 0 ou à 1; on aura aussi

$$d' = 2d'' + \varepsilon,$$

$$V = \begin{bmatrix} (2a''+\varepsilon)n^2+1 & 2b'n^2 \\ 2c'n^2 & (2d''+\varepsilon)n^2+1 \end{bmatrix},$$

c'est-à-dire

$$V \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2n^2}$$

ou bien encore

$$V \equiv \begin{pmatrix} n^2+1 & 0 \\ 0 & n^2+1 \end{pmatrix} \quad (\mathrm{mod}\, 2n^2).$$

Les substitutions V définissent un sous-groupe homogène d'indice $\mu(2n^2)$. Donc :

Pour n pair les substitutions de Γ *qui laissent invariables toutes les* $\sigma_{hk}u$ *forment un sous-groupe homogène* $\Gamma_{\mu(2n^2)}$.

136. Un problème d'un autre genre consiste à rechercher les substitutions de Γ laissant invariable une fonction $\sigma_{hk}u$ particulière.

Pour cela formons tout d'abord l'équation de périodicité de σ_{hk} relative aux indices.

La relation (6) (n° 134) donne

$$(1) \qquad \sigma_{h+pn,\,k+qn}u = e^{\left(\frac{2\pi}{n}+2\eta'\right)\left(u-\frac{z}{n}-z'\right)}\sigma\left(u-\frac{2z}{n}-2z'\right),$$

η, z ayant la même signification qu'au n° 134, avec

$$\eta' = p\eta_1 + q\eta_2, \qquad z' = pz_1 + qz_2.$$

D'autre part, d'après la formule (2) (n° 134)

$$(2) \qquad \sigma\left(u-\frac{2z}{n}-2z'\right) = (-1)^{pq+p+q}e^{-2\eta'\left(u-\frac{2z}{n}-z'\right)}\sigma\left(u-\frac{2z}{n}\right);$$

de plus (6) peut s'écrire

$$(3) \qquad \sigma\left(u-\frac{2z}{n}\right) = e^{-\frac{2\eta}{n}\left(u-\frac{z}{n}\right)}\sigma_{hk}u.$$

Multiplions membre à membre (1), (2), (3) et observons que d'après (3) (n° 134) on a

$$\eta'z - \eta z' = \frac{\pi i}{2}(-pk+qh),$$

il vient

$$(4) \qquad \sigma_{h+pn,\,k+qn} = (-1)^{pq+p+q}e^{-\frac{\pi i}{n}(pk-qh)}\sigma_{hk}u,$$

qu'on peut écrire encore

$$(5) \qquad \sigma_{h+pn,\,k+qn}u = (-1)^{p^2+pq+q^2}e^{-\frac{\pi i}{n}(pk-qh)}\sigma_{hk}u.$$

Cette relation montre que si l'on ajoute aux indices de $\sigma_{hk}u$ des multiples de n la fonction se reproduit multipliée par un facteur constant qui est une racine de l'unité. Il suffit donc de considérer les fonctions $\sigma_{hk}u$ dans lesquelles les h, k ne sont ni l'un ni l'autre congrus à n.

Voici une autre formule importante.

Soient α, β, γ, δ les éléments d'une substitution modulaire quelconque, les formules (1) et (7) du n° 134 donnent

$$(6) \qquad \sigma_{h\alpha+k\gamma,\, h\beta+k\delta}(z_1, z_2) = \sigma_{hk}(\alpha z_1 + \beta z_2, \gamma z_1 + \delta z_2).$$

Cela posé, si une substitution modulaire $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ change $\sigma_{hk}(z_1, z_2)$ en elle-même, c'est-à-dire si l'on a identiquement

$$\sigma_{hk}(\alpha z_1 + \delta z_2, \gamma z_1 + \delta z_2) = \sigma_{hk}(z_1, z_2),$$

on aura aussi, en tenant compte de (6),

$$\sigma_{h\alpha+k\gamma,\, h\beta+k\delta}(z_1, z_2) = \sigma_{hk}(z_1, z_2).$$

Il suit de là

$$h\alpha + k\gamma = h, \qquad h\beta + k\delta = k;$$

d'où successivement

$$\frac{h}{k} = \frac{-\gamma}{\alpha - 1} = \frac{\delta - 1}{\beta},$$

$$(\alpha - 1)(\delta - 1) - \beta\gamma = 0,$$

et comme

$$\alpha\delta - \beta\gamma = 1,$$

on obtient finalement

$$\alpha + \delta = 2.$$

Donc la substitution considérée est parabolique (n° 25).

Posons

$$\alpha = 1 + \theta,$$

d'où

$$\delta = 1 - \theta;$$

soit d le plus grand commun diviseur de h, k, posons $h = dh'$, $k = dk'$; on aura

$$\frac{h'}{k'} = \frac{-\gamma}{\theta} = \frac{\theta}{\beta}$$

et, en désignant par d et p deux entiers,

$$-\gamma = \lambda h', \qquad \theta = \lambda k' = \mu h', \qquad \beta = \mu k'.$$

De la relation $\lambda k' = \mu h'$ il suit, h' et k' étant premiers entre eux,

$$\lambda = rh', \qquad \mu = rk',$$

d'où

$$\alpha = 1 + rh'k', \qquad \beta = rk'^2, \qquad \gamma = -rh'^2, \qquad \delta = 1 - rh'k'.$$

La substitution considérée $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est donc la puissance d'ordre r de la substitution parabolique d'amplitude 1

$$V = \begin{pmatrix} 1 + h'k' & k'^2 \\ -h'^2 & 1 - h'k' \end{pmatrix}.$$

Supposons que les trois nombres h, k, n soient premiers entre eux.

Alors deux puissances de V seront congrues à n, s'il en est de même de leurs exposants, et dans ce cas seulement. En effet si $V^s \equiv V^t$, c'est-à-dire si

$$1 + sh'k' \equiv 1 + th'k', \qquad sk'^2 \equiv tk'^2,$$
$$-sh'^2 \equiv -th'^2, \qquad 1 - sh'k' \equiv 1 - th'k' \qquad (\text{mod } n),$$

on conclut nécessairement, d'après l'hypothèse,

$$s \equiv t \qquad (\text{mod } n);$$

et réciproquement si cette dernière relation a lieu, il en est de même des précédentes et l'on a $V^s \equiv V^t$.

Donc les seules puissances de V qui soient distinctes sont

$$1, \quad V, \quad V^2, \quad \ldots, \quad V^{n-1}.$$

En combinant ces dernières substitutions avec celles qui laissent invariables toutes les σ_{hk}, on obtient toutes les substitutions qui laissent invariable la fonction particulière σ_{hk} considérée.

Les sous-groupes ainsi formés sont équivalents, puisque le sous-groupe formé des substitutions qui laissent invariables toutes les σ_{hk}, est un sous-groupe invariant; et les sous-groupes tels que

$$1, \quad V, \quad V^2, \quad \ldots, \quad V^{n-1}$$

sont tous équivalents, car cette propriété appartient à toutes les substitutions paraboliques ayant *un* pour amplitude (nº 97).

Proposons-nous de déterminer le nombre des fonctions σ_{hk}, pour lesquelles h, k, n sont premiers entre eux.

Soit p_1 un facteur premier de n. Pour former un couple de nombres h, k plus petits que n et ne renfermant pas tous deux le facteur p_1, on peut combiner un des $\frac{n}{p_1}$ nombres inférieurs à n et divisibles par p_1 avec un des $\left(n - \frac{n}{p_1}\right)$ autres nombres restants, ou bien un de ces derniers avec un quelconque des nombres inférieurs à n, de sorte qu'on a en tout

$$\frac{n}{p_1}\left(n - \frac{n}{p_1}\right) + \left(n - \frac{n}{p_1}\right) n = n^2\left(1 - \frac{1}{p_1^2}\right)$$

combinaisons. Or si p_2 est un facteur premier de n, autre que p_1, parmi les $\frac{n}{p_1}$, $\left(n - \frac{n}{p_1}\right)$ et n nombres considérés, il y en a respectivement

$$\frac{n}{p_1 p_2}, \quad \frac{1}{p_2}\left(n - \frac{n}{p_1}\right), \quad \frac{n}{p_2}$$

divisibles par p_2, en sorte que, parmi les combinaisons formées, il y en aura

$$\frac{n}{p_1 p_2^2}\left(n - \frac{n}{p_1}\right) + \left(n - \frac{n}{p_1}\right)\frac{n}{p_2^2} = \frac{n^2}{p_2^2}\left(1 - \frac{1}{p_1^2}\right)$$

constituées par deux nombres divisibles par p_2. Il reste donc

$$n^2\left(1 - \frac{1}{p_2^1}\right) - \frac{n^2}{p_2^2}\left(1 - \frac{1}{p_1^2}\right) = n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)$$

combinaisons de deux nombres n'ayant pour facteur commun ni p_1, ni p_2. En continuant de la sorte, on trouve que le nombre des combinaisons de deux nombres h, k inférieurs à n, et tels que h, k, n n'aient aucun facteur commun est

$$(7) \qquad n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)\cdots\left(1 - \frac{1}{p_r^2}\right),$$

$p_1, p_2, \ldots, p_r$ étant les différents facteurs premiers de n.

Posons

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \quad [1]$$

[1] On sait que dans la théorie des nombres la notation $\varphi(n)$ indique combien il y a de nombres inférieurs à n et premiers avec n.

et

$$\psi(n) = n\left(1+\frac{1}{p_1}\right)\left(1+\frac{1}{p_2}\right)\cdots\left(1+\frac{1}{p_r}\right).$$

Alors l'expression (7) peut s'écrire

$$\varphi(n)\,\psi(n),$$

d'où

$$\mu(n) = \frac{n}{2}\varphi(n)\,\psi(n).$$

Calculons maintenant le nombre des sous-groupes équivalents au sous-groupe, qui laisse invariable l'une des σ_{hk}.

Ce dernier sous-groupe a été obtenu en combinant V et ses puissances avec le sous-groupe qui laisse invariable toutes les σ_{hk} et qui se compose de substitution toutes congrues à *un*, suivant le module n. Par suite au sous-groupe considéré de Γ correspondra dans $G_{\mu(n)}$ le sous-groupe $(I, V, V^2, \ldots, V^{n-1})$.

Pour résoudre le problème proposé, nous chercherons donc à déterminer le plus grand sous-groupe de $G_{\mu(n)}$ admettant $(1, V, \ldots, V^{n-1})$ comme sous-groupe invariant.

Considérons, pour simplifier la fonction σ_{01} (¹), dans le cas actuel

$$h = 0, \qquad k = 1,$$

d'où

$$h' = 0, \qquad k' = 1$$

et

$$V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = S.$$

Si

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

est permutable avec le groupe $(1, S, S^2, \ldots, S^{n-1})$ on a

$$U^{-1}SU = S^r,$$

c'est-à-dire

$$\begin{pmatrix} 1-\alpha\gamma & \alpha^2 \\ -\gamma^2 & 1+\alpha\gamma \end{pmatrix} \equiv \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \qquad (\mathrm{mod}\ n);$$

(¹) Il est à peine besoin de dire que le raisonnement s'étend à n'importe quel couple de valeurs h, k.

d'où il suit

$$\left.\begin{aligned} &(8) \qquad 1-\alpha\gamma \equiv \pm 1 \\ &(9) \qquad 1+\alpha\gamma \equiv \pm 1 \\ &(10) \qquad \gamma^2 \equiv 0 \end{aligned}\right\} \pmod{n}.$$

En faisant la somme des congruences (8) et (9), on obtient

$$2 \equiv \pm 2 \pmod{n},$$

en sorte que, si $n > 4$, on doit prendre le signe $+$, et la relation (8) montre que

$$(11) \qquad \alpha\gamma \equiv 0 \pmod{n}.$$

Multiplions la congruence (11) par δ, puis (10) par $-\beta$ et sommons; nous aurons, en tenant compte de $\alpha\delta - \beta\gamma = 1$,

$$\gamma \equiv 0 \pmod{n},$$

d'où

$$\alpha\delta \equiv 1 \pmod{n}.$$

On peut donc donner à α une quelconque des $\varphi(n)$ valeurs non congrues à n et premières avec n; pour chacune d'elles δ est déterminé, et β peut prendre n valeurs.

Par conséquent, le nombre des substitutions U permutables avec S est $n\varphi(n)$; elles se réduisent à $\frac{1}{2}n\varphi(n)$, car on peut considérer comme égales deux substitutions dont les éléments sont égaux et opposés. Par suite, le nombre des sous-groupes distincts équivalents au sous-groupe qui laisse invariable l'une des σ_{hk} est $\mu(n) : \frac{1}{2}n\psi(n)$, c'est-à-dire $\psi(n)$.

Donc : *Les fonctions σ_{hk}, pour lesquels h, k, n n'ont aucun diviseur commun, sont au nombre de $\varphi(n)\psi(n)$ et se partagent en $\psi(n)$ systèmes, chacun d'eux comprenant $\varphi(n)$ fonctions invariantes dans un même sous-groupe de* Γ (1).

---

(1) Ces conclusions ont encore lieu pour $n = 3$; il en est de même pour $n = 2$, car alors il est indifférent de prendre le signe $+$ ou le signe $-$ dans les relations (8) et (9). Pour $n = 4$, outre les substitutions formées à l'aide du raisonnement précédent, il en existe deux autres qu'on obtient en prenant le signe $-$ dans les équations (8) et (9), ce qui donne

$$\alpha = 1, \qquad \beta = \begin{cases} 0 \\ 2 \end{cases}, \qquad \gamma = 2, \qquad \delta = 1.$$

Supposons maintenant que h, k, n aient un diviseur commun t. Posons

$$h = th', \qquad k = tk', \qquad n = tn'.$$

La formule (6) (n° 134) donne

$$\sigma_{hk}(u \mid z_1, z_2) = e^{\frac{2h'\eta_1 + 2k'\eta_2}{n'}\left(u - \frac{h'z_1 + k'z_2}{n'}\right)} \sigma\left(u - \frac{2h'z_1 + 2k'z_2}{n'} \,\middle|\, z_1, z_2\right),$$

en sorte que dans le cas considéré, σ_{hk} peut être regardée comme une fonction $\sigma_{h'k'}$ relative au diviseur n'. Donc :

Les σ_{hk}, pour lesquels h, k, n ont un plus grand commun diviseur $t > 1$, sont au nombre de $\varphi\left(\frac{n}{t}\right)\psi\left(\frac{n}{t}\right)$, et se partagent en $\psi\left(\frac{n}{t}\right)$ systèmes, chacun d'eux comprenant $\varphi\left(\frac{n}{t}\right)$ fonctions invariantes dans un même sous-groupe de Γ.

137. Les puissances $n^{\text{ièmes}}$ des σ_{hk} sont aussi des fonctions invariantes dans certains sous-groupes de Γ.

Pour n impair, les formules (2) (n° 135) donnent

$$(\sigma'_{hk}u)^n = e^{(n-1)\pi i[-h^2b + hk(a-d) + k^2c]}[\sigma_{hk}u]^n,$$

c'est-à-dire puisque $n - 1$ est pair

$$(\sigma'_{hk}u)^n = (\sigma_{hk}u)^n.$$

Pour n pair, les formules (9) (n° 134) donnent immédiatement

$$(\sigma'_{hk}u)^{2n} = (\sigma_{hk}u)^{2n}.$$

Donc les substitutions $V \equiv 1 \pmod{n}$ laissent invariables les fonctions $(\sigma_{hk}u)^{2n}$ et, dans le cas où n est impair, les fonctions $(\sigma_{hk}u)^n$.

138. Les fonctions σ_{hk} considérées jusqu'à présent sont des fonctions homogènes, ou comme on dit encore des *formes*, de z_1, z_2, de degré 1.

Rappelons la formule

$$(1) \qquad \sigma u = \frac{2z_2}{\pi} e^{\frac{\eta_2 u^2}{2z_2}} \sin\frac{\pi u}{2z_2} \prod_{j=1}^{\infty}\left(1 - \frac{\sin^2\frac{\pi u}{2z_2}}{\sin^2\frac{j\pi z_1}{z_2}}\right).$$

Posons, comme plus haut,

$$h\eta_1 + k\eta_2 = \eta, \qquad hz_1 + kz_2 = z,$$

nous aurons, d'après la formule (7) (n° 134),

$$\sigma_{hk}(z_1, z_2) = -e^{-\frac{2\eta_1 z}{n^2}} \frac{2z_2}{\pi} e^{\frac{2\eta_2 z^2}{n^2 z_2}} \sin\frac{\pi z}{nz_2} \prod_{j=1}^{\infty}\left(1 - \frac{\sin^2\frac{\pi z}{nz_2}}{\sin^2\frac{j\pi z_1}{z_2}}\right)$$

ou, tenant compte de (3) (n° 134),

$$(1) \qquad \sigma_{hk}(z_1, z_2) = -\frac{2z_2}{\pi} e^{\frac{h\pi i z}{n^2 z_2}} \sin\frac{\pi z}{nz_2} \prod_{j=1}^{\infty}\left(1 - \frac{\sin^2\frac{\pi z}{nz_2}}{\sin^2\frac{j\pi z_1}{z_2}}\right).$$

Comme on le voit, à l'exception du facteur z_2, toutes les autres dépendent uniquement du rapport $\frac{z_1}{z_2}$; c'est ce que nous voulions établir.

En conséquence, si l'on prend les quotients de puissances égales des σ_{hk}, on aura des fonctions de $\frac{z_1}{z_2}$, invariantes dans certains sous-groupes de Γ, c'est-à-dire des fonctions modulaires.

139. Pour de ne pas dépasser les limites du cadre assigné à cet Ouvrage, nous n'appliquerons les théories précédentes qu'à un seul exemple, le plus simple de tous, celui des fonctions invariantes dans le sous-groupe Γ_6. Ici $n = 2$; les fonctions σ_{hk}^4 sont des formes invariantes, et leurs rapports sont des fonctions invariantes.

Nous nous proposons d'exprimer, à l'aide de ces fonctions invariantes, une fonction invariante λ, que nous allons définir.

Nous savons (n° 131) que si Z, z et z' sont liées par les relations

$$(1) \qquad Z = \frac{(z'^3+1)^2}{4z'^3}, \qquad Z = J(z),$$

z' est une fonction uniforme de z, ou, d'une façon plus précise, une fonction modulaire appartenant au sous-groupe Γ_6.

Il en est de même si, au lieu des relations (1), on considère les relations

$$(2) \qquad Z' = \frac{(z'^3+1)^2}{z'^3}, \qquad Z = J(z),$$

Z et Z' étant exprimables rationnellement l'un par l'autre, c'est-à-dire liés par une relation linéaire.

Nous supposerons

$$(3) \qquad Z' = \frac{Z - 1}{Z},$$

de plus, au lieu de z' nous introduirons une fonction linéaire de z'. Ce sera encore une fonction modulaire du groupe Γ_6.

Soit

$$(4) \qquad z' = \frac{\lambda + e^{\frac{4\pi i}{3}}}{\lambda + e^{\frac{2\pi i}{3}}} = \frac{\lambda + \frac{-1 - i\sqrt{3}}{2}}{\lambda + \frac{-1 + i\sqrt{3}}{2}}$$

la relation que nous établissons entre z' et λ.

En tenant compte de (3) et (4), la première des relations (2) devient

$$\frac{Z - 1}{Z} = \frac{(2\lambda^3 - 3\lambda^2 - 3\lambda + 2)^2}{4(\lambda^2 - \lambda + 1)^3}.$$

On en déduit facilement

$$Z = \frac{4(\lambda^2 - \lambda + 1)^3}{27\lambda^2(\lambda - 1)^2},$$

qu'on peut écrire

$$Z - 1 : Z : 1 = (2\lambda^3 - 3\lambda^2 - 3\lambda + 2)^2 : 4(\lambda^2 - \lambda + 1)^3 : 27\lambda^2(\lambda - 1)^2$$

ou encore, Z étant égal à J,

$$27 g_3^2 : g_2^3 : \Delta - (2\lambda^3 = 3\lambda^2 - 3\lambda + 2)^2 : 4(\lambda^2 - \lambda + 1)^3 : 27\lambda^2(\lambda - 1)^2.$$

Ces formules montrent que les valeurs de λ, correspondant à $J = \infty$, sont $\lambda = 1, 0, \infty$. Or, les nœuds du réseau de Γ_6 sont des points de l'axe réel, c'est-à-dire des points homologues dans Γ du point à l'infini; d'autre part pour $z = \infty$ on a $J = \infty$, donc en tous les nœuds du réseau de Γ_6, on a $J = \infty$, et par suite en ces nœuds λ prend les trois valeurs 1, 0, ∞. Comme parmi les nœuds du réseau considéré figurent les points $z = 1, 0, \infty$, on voit qu'aux valeurs 1, 0, ∞ de z correspondent dans un certain ordre les valeurs 1, 0, ∞ de λ. Cet ordre est arbitraire; car z', et par suite λ, n'a pas été défini d'une façon unique, mais seulement comme racine d'une équation algébrique. En fixant cet ordre d'une certaine manière on définira λ sans ambiguïté.

Nous adopterons la correspondance suivante

$$(5)\qquad \lambda(1) = 1, \qquad \lambda(0) = 0, \qquad \lambda(\infty) = \infty.$$

Si l'on fait subir à z une substitution modulaire, λ devient une autre racine de l'équation entre J et λ; mais Γ_6 étant de genre zéro (n° 98), toutes les racines de l'équation sont des fonctions linéaires de l'une quelconque d'entre elles (n° 133, a). En d'autres termes, à chaque substitution modulaire de z correspond une substitution linéaire de λ.

Cherchons les substitutions linéaires de λ correspondant aux substitutions S, T de z.

Soient

$$\mathbf{S} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \mathbf{T} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

ces substitutions, de sorte que

$$(6)\qquad \lambda(z+1) = \frac{a\lambda(z)+b}{c\lambda(z)+d}, \qquad \lambda\left(-\frac{1}{z}\right) = \frac{a'\lambda(z)+b'}{c'\lambda(z)+d'}.$$

Remplaçons dans ces relations z successivement par 1, 0, ∞, en tenant compte de (5) et observant que

$$\lambda(z) = \lambda(0), \qquad \lambda(-1) = \lambda(1),$$

nous aurons

$$0 = \frac{a+b}{c+d}, \qquad 1 = \frac{b}{d}, \qquad \infty = \frac{a}{c},$$

$$1 = \frac{a'+b'}{c'+d'}, \qquad \infty = \frac{b'}{d'}, \qquad 0 = \frac{a'}{c'},$$

d'où

$$a = -b = -d, \qquad c = 0; \qquad a' = d' = 0. \qquad b' = c',$$

en sorte qu'on peut poser

$$\mathbf{S} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

et les relations (6) deviennent

$$\lambda(z+1) = -\lambda(z) + 1, \qquad \lambda\left(-\frac{1}{z}\right) = \frac{1}{\lambda(z)}.$$

Les substitutions **S**, **T** engendrent un groupe holoédriquement isomorphe au groupe G_6, c'est-à-dire un groupe diédrique. Les

6 substitutions de ce groupe sont

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{S} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\mathbf{ST} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad \mathbf{TS} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{STS} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

Ainsi, en désignant simplement par λ une des valeurs de λ correspondant à une valeur déterminée de J, les 6 valeurs de λ correspondantes, c'est-à-dire les 6 racines de l'équation

$$J = \frac{4(\lambda^2 - \lambda + 1)^3}{27\lambda^2(\lambda - 1)^2},$$

seront

$$\lambda, \quad -\lambda + 1, \quad \frac{1}{\lambda}, \quad \frac{1}{-\lambda+1}, \quad \frac{\lambda - 1}{\lambda}, \quad \frac{\lambda}{\lambda - 1}.$$

Posons

$$\lambda = \frac{\lambda_1}{\lambda_2},$$

et donnons à λ_1, λ_2 la signification plus précise suivante :

$$(7) \qquad \lambda_1 = -e^{\frac{\pi i}{4}} \frac{2z_2}{\sqrt{\pi}} \frac{\lambda}{\sqrt{\lambda'}}, \qquad \lambda_2 = -e^{\frac{\pi i}{4}} \frac{2z_2}{\sqrt{\pi}} \frac{1}{\sqrt{\lambda'}},$$

λ' représentant la dérivée de λ par rapport à z.

Nous aurons

$$27g_3^2 : g_2^3 : \Delta$$
$$= (2\lambda_1^3 - 3\lambda_1^2\lambda_2 - 3\lambda_1\lambda_2^2 - 2\lambda_2^3)^2 : 4(\lambda_1^2 - \lambda_1\lambda_2 + \lambda_2^2)^3 : 27\lambda_1^2\lambda_2^2(\lambda_1 - \lambda_2)^2,$$

ou bien, en désignant par h un facteur que nous déterminerons plus loin

$$(8) \qquad \begin{cases} 27hg_3^2 = (2\lambda_1^3 - 3\lambda_1^2\lambda_2 - 3\lambda_1\lambda_2^2 + 2\lambda_2^3)^2, \\ hg_2^3 = 4(\lambda_1^2 - \lambda_1\lambda_2 + \lambda_2^2)^3, \\ h\Delta = 27\lambda_1^2\lambda_2^2(\lambda_1 - \lambda_2)^2. \end{cases}$$

Puisque λ_1, λ_2 sont des formes du premier degré en z_1, z_2, tandis que g_2, g_3, Δ sont respectivement (nº 129) de degrés -4, -6, -12, il en résulte que h est une forme du 18e degré.

Pour déterminer cette forme, il faut trouver les substitutions linéaires et homogènes que subissent λ_1 et λ_2, quand λ subit les substitutions **S**, **T**.

Soit, en général, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la substitution subie par λ, quand on applique à z la substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, on aura

$$(9) \qquad \lambda\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)=\frac{a\lambda(z)+b}{c\lambda(z)+d}.$$

En dérivant, il vient (dans l'hypothèse $\alpha\delta-\beta\delta=1$)

$$\frac{1}{(\gamma z+\delta)^2}\lambda'\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)=\frac{ad-bc}{[c\lambda(z)+d]^2}\lambda'(z)$$

ou bien

$$(10) \qquad \pm\frac{\sqrt{ad-bc}\,(\gamma z+\delta)}{\sqrt{\lambda'\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)}}=\frac{c\lambda(z)+d}{\sqrt{\lambda'(z)}}.$$

Or, la seconde des relations (7) donne

$$\lambda_2(\alpha z_1+\beta z_2,\ \gamma z_1+\delta z_2)=-e^{\frac{\pi i}{4}}\frac{2}{\sqrt{\pi}}(\gamma z_1+\delta z_2)\frac{1}{\sqrt{\lambda'\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)}}$$

et, par suite, il vient pour (10), en tenant compte de (7),

$$(11) \qquad \pm\sqrt{ad-bc}\,\lambda_2(\alpha z_1+\beta z_2,\ \gamma z_1+\delta z_2)=c\lambda_1(z_1,z_2)+d\lambda_2(z_1,z_2),$$

et enfin, pour (9),

$$(12) \qquad \pm\sqrt{ad-bc}\,\lambda_1(\alpha z_1+\beta z_2,\ \gamma z_1+\delta z_2)=a\lambda_1(z_1,z_2)+b\lambda_2(z_1,z_2).$$

Les formules (11) et (12) donnent les deux substitutions homogènes correspondant à la substitution non homogène (9).

En particulier, aux substitutions non homogènes **S**, **T** correspondent les substitutions homogènes suivantes, que nous désignerons par les mêmes lettres :

$$\mathbf{S}\begin{cases}\pm i\lambda_1(z_1+z_2,\ z_2)=-\lambda_1(z_1,z_2)+\lambda_2(z_1,z_2)\\ \pm i\lambda_2(z_1+z_2,\ z_2)=\lambda_2(z_1,z_2)\end{cases},$$

$$\mathbf{T}\begin{cases}\pm i\lambda_1(-z_2,\ z_1)=\lambda_2(z_1,z_2)\\ \pm i\lambda_2(-z_2,\ z_1)=\lambda_1(z_1,z_2)\end{cases}.$$

Pour donner à ces formules une forme plus concise désignons respectivement par λ'_i λ''_i les transformées de λ_i par les substitu-

tions **S**, **T**, nous aurons

$$\mathbf{S}\left\{\begin{array}{l}\pm i\lambda'_1 = -\lambda_1 + \lambda_2\\ \pm i\lambda'_2 = \lambda_2\end{array}\right., \qquad \mathbf{T}\left\{\begin{array}{l}\pm i\lambda''_1 = \lambda_2\\ \pm i\lambda''_2 = \lambda_1\end{array}\right..$$

Il est facile de vérifier que **S** et **T** transforment en elle-même la forme $[\lambda_1\lambda_2(\lambda_1 - \lambda_2)]^4$, qui est, par suite, une forme modulaire principale, et comme cela a lieu également pour Δ, il en sera de même pour le produit

$$3^6\Delta[\lambda_1\lambda_2(\lambda_1 - \lambda_2)]^4,$$

mais ce produit est de degré zéro; c'est donc une fonction principale, c'est-à-dire une fonction rationnelle de J. D'autre part, il résulte de la dernière équation (8)

$$(13) \qquad 3^6\Delta[\lambda_1\lambda_2(\lambda_1 - \lambda_2)]^4 = h^2\Delta^3,$$

en sorte que $h^2\Delta^3$ est une fonction modulaire principale, donc une fonction rationnelle de J, soit $\rho(J)$, que nous nous proposons de déterminer.

Dans ce but, observons tout d'abord que si l'on représente sur un plan les valeurs de la fonction $\lambda(z)$, et que sur ce plan l'on construise la surface de Riemann, dont chaque feuillet correspond à un bitriangle du réseau Γ_6, les points de ramification de cette surface correspondront aux nœuds du réseau considéré, et par conséquent c'est seulement en ces nœuds qu'on aura

$$\lambda'(z) = 0.$$

Il suit de là que $\lambda'(z)$ n'est jamais nulle en des points extérieurs à l'axe réel.

Or, comme dans le réseau modulaire, le seul point du triangle fondamental où $\lambda = \infty$ est le point à l'infini, λ_1 et λ_2 auront des valeurs finies pour toute valeur finie de z située dans ce triangle. On peut en dire autant de Δ, comme cela résulte de son expression; et dans le réseau modulaire, le seul point du triangle fondamental, où la fonction (13) pourrait devenir infinie, est le point à l'infini. Or, on a $\tau = 0$ pour $z = i\infty$ (n° 129) et les valeurs approchées de g_2, g_3, Δ pour $z = i\infty$ sont (*voir* les formules du n° 129)

$$g_2 = \frac{1}{12}\left(\frac{\pi}{z_2}\right)^4, \qquad g_3 = \frac{1}{216}\left(\frac{\pi}{z_2}\right)^6, \qquad \Delta = \left(\frac{\pi}{z_2}\right)^{12}\tau;$$

d'où

$$J = \frac{g_2^3}{\Delta} = \frac{1}{12^3\tau}.$$

D'autre part

$$J = \frac{4}{27} \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2},$$

d'où la formule approchée

$$J = \frac{4}{27} \lambda^2$$

ou bien

$$\lambda = \sqrt{\frac{27 J}{4}} = \frac{1}{16\sqrt{\tau}}.$$

Prenant la dérivée et remarquant que $\frac{d\tau}{dz} = 2\pi i \tau$, il vient

$$\lambda' = -\frac{\pi i}{16\sqrt{\tau}},$$

puis, d'après (7),

$$\lambda_1 = \frac{i z_2}{2\pi \sqrt[4]{\tau}}, \qquad \lambda_2 = \frac{8 i z_2}{\pi} \sqrt[4]{\tau},$$

d'où

$$\lambda_1 \lambda_2 (\lambda_1 - \lambda_2) = -\frac{2 i z_2^3}{\pi^3 \sqrt[4]{\tau}},$$

et enfin

$$\rho(J) = 3^6 \Delta [\lambda_1 \lambda_2 (\lambda_1 - \lambda_2)]^4 = 3^6 . 2^4.$$

Donc, la fonction considérée ne devient infinie en aucun point du triangle fondamental, par suite en aucun point du plan; elle se réduit par conséquent à une constante qui est précisément $3^6 . 2^4$. On a ensuite

$$h = \frac{108}{\Delta^{\frac{3}{2}}}$$

et les formules (8) deviennent

$$(14) \quad \begin{cases} 2\lambda_1^3 - 3\lambda_1^2 \lambda_2 - 3\lambda_1 \lambda_2^2 + 2\lambda_2^3 = \dfrac{54 g_3}{\Delta^{\frac{3}{4}}}, \\ \lambda_1^2 - \lambda_1 \lambda_2 + \lambda_2^2 = \dfrac{3 g_2}{\Delta^{\frac{1}{2}}}, \\ \lambda_1 \lambda_2 (\lambda_1 - \lambda_2) = \dfrac{2}{\Delta^{\frac{1}{4}}}. \end{cases}$$

Posons

$$\mu = -\frac{\lambda_2}{\sqrt[4]{\Delta}} = -\frac{1}{2} \lambda_1 \lambda_2^2 (\lambda_1 - \lambda_2) = \frac{8 z_2^4}{\pi^2} \frac{\lambda(\lambda - 1)}{\lambda'^2}.$$

Comme λ' reste invariable par les mêmes substitutions que λ, $\frac{\mu}{z_2^4}$ est une fonction modulaire du sous-groupe Γ_6. D'autre part, σ_{01}^4 est une forme modulaire de degré 4 du même groupe, de sorte que $\frac{\sigma_{01}^4}{z_2^4}$ est une fonction modulaire.

De même $\theta = \frac{\sigma_{01}^4}{\mu}$ est une fonction modulaire du groupe Γ_6.

Je dis que σ_{01} et μ restent tous deux invariables par la substitution S.

En effet, tout d'abord, en faisant dans la formule (1) (n° 138)

$$h = 0, \qquad k = 1, \qquad n = 2,$$

on obtient

$$\sigma_{01} = -\frac{2z_2}{\pi} \prod_{j=1}^{\infty} \left(1 - \frac{1}{\sin^2 \frac{j\pi z_1}{z_2}}\right),$$

et il est facile de voir que σ_{01} reste invariable par la substitution homogène S

$$z'_1 = z_1 + z_2, \qquad z'_2 = z_2.$$

Quant à μ, on peut remarquer que si l'on applique à z_1, z_2 la substitution S, λ subit la substitution linéaire correspondante $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$, de sorte que

$$\lambda(z+1) = -\lambda(z) + 1,$$

d'où

$$\lambda'(z+1) = -\lambda'(z)$$

et, par suite,

$$\mu(z_1 + z_2, z_2) = \frac{8z_2^4}{\pi^2} \frac{\lambda(z+1)[\lambda(z+1) - 1]}{\lambda'^2(z+1)}$$
$$= \frac{8z_2^4}{\pi^2} \frac{[-\lambda(z) + 1][-\lambda(z)]}{[-\lambda'(z)]^2} = \mu(z_1, z_2).$$

Donc la fonction $\theta = \frac{\sigma_{01}^4}{\mu}$ est invariante par la substitution S. Si maintenant nous considérons la partie d'un champ fondamental de Γ_6 comprise entre deux droites parallèles à l'axe des y, distantes entre elles de la longueur 1, θ prendra dans cette aire toutes les valeurs dont elle est susceptible. Prenons, en particulier, pour champ fondamental celui de la figure 29 (p. 135), et comme bande, la bande comprise entre les droites d'abscisse $\pm\frac{1}{2}$. Dans ce champ, θ, si

elle ne se réduit pas à une constante, doit prendre la valeur ∞. On peut en dire autant de $\frac{1}{\theta}$. Donc θ doit prendre aussi la valeur o. Or, on peut démontrer que dans le champ considéré, excepté aux points $z = 0$, $z = i\infty$, θ ne peut devenir ni nulle, ni infinie. La fonction σ_{01}, comme cela résulte de son expression, est toujours finie et différente de zéro pour toutes les valeurs finies et complexes de $\frac{z_1}{z_2}$; d'autre part, puisque pour z fini et différent de zéro, Δ et λ_2 sont finis et différents de zéro, il en est de même pour μ : c'est ce que nous voulions établir.

Il suit de là qu'au point $z = i\infty$, θ doit être nulle ou infinie.

Calculons maintenant directement la valeur approchée de θ au point à l'infini. Puisque

$$\lim_{z=i\infty} \sin z = i\infty,$$

on a, comme expression approchée de σ_{01},

$$\sigma_{01} = -\frac{2z_2}{\pi}.$$

D'autre part, les expressions approchées de λ, λ' donnent

$$\mu = -\frac{8z_2^4}{\pi_4},$$

d'où

$$\theta = \frac{\sigma_{01}^4}{\mu} = -2,$$

ce qui prouve que θ se réduit à une constante, de sorte que

$$\sigma_{02}^4 = -2\mu.$$

Faisons maintenant, dans les formules (6) (n° 136),

$$h = 0, \qquad k = 1, \qquad \alpha = 0, \qquad \beta = -1, \qquad \gamma = 1, \qquad \delta = 0;$$

nous aurons

$$\sigma_{10}(z_1, z_2) = \sigma_{01}(-z_2, z_1),$$

relation qui exprime que, par la substitution T, σ_{01} se change en σ_{10}. D'autre part T change λ_2 et λ_1 respectivement en $\pm i\lambda_1$, $\pm i\lambda_2$, ce qui montre d'après la dernière formule (14), que $\Delta^{\frac{1}{4}}$ se

transforme en $\mp i\Delta^{\frac{1}{4}}$. Il suit de là que

$$\mu = -\frac{\lambda_2}{\Delta^{\frac{1}{4}}}$$

se transforme en

$$-\nu = +\frac{\lambda_1}{\Delta^{\frac{1}{4}}},$$

de sorte qu'on obtient la relation

$$\frac{\sigma_{10}^4}{\nu} = 2.$$

En la combinant avec

$$\sigma_{01}^4 = -2\mu$$

trouvée plus haut, on obtient

$$\frac{\mu}{\nu} = -\frac{\sigma_{01}^4}{\sigma_{10}^4}$$

ou bien

$$\lambda = -\frac{\sigma_{10}^4}{\sigma_{01}^4}.$$

Nous sommes donc parvenus à exprimer λ à l'aide des formes modulaires du sous-groupe homogène Γ_6.

On peut, au moyen de l'expression trouvée, donner facilement une interprétation géométrique de la fonction λ.

On sait que si z_i est une des demi-périodes z_1, z_2, z_3 $(z_3 = -z_1 - z_2)$ on a

$$p u - p z_i = -\frac{\sigma(u + z_i)\sigma(u - z_i)}{\sigma^2 u \sigma^2 z_i}.$$

D'ailleurs

$$\sigma(u - z_i) = -e^{-2\eta_i u}\sigma(u + z_i),$$

donc on peut écrire

$$p u - p z_i = e^{-2\eta_i u}\frac{\sigma^2(u + z_i)}{\sigma^2 u \sigma^2 z_i}.$$

Donnons à i successivement les valeurs 1 et 2, faisons $u = z_i$, divisons membre à membre les deux équations résultantes, et posons comme d'habitude

$$p z_i = e_i,$$

nous aurons

$$\frac{e_3 - e_2}{e_3 - e_1} = e^{2(\eta_1 - \eta_2)z_3}\frac{\sigma^2 z_1 \sigma^2(z_2 + z_3)}{\sigma^2 z_2 \sigma^2(z_1 + z_3)}.$$

Or, σu est une fonction impaire, de sorte que

$$\sigma(z_2 + z_3) = \sigma(-z_1) = -\sigma z_1,$$
$$\sigma(z_1 + z_3) = \sigma(-z_2) = -\sigma z_2,$$

de plus, d'après la formule (3) (n° 134),

$$\begin{aligned}(\eta_1 - \eta_2) z_3 &= (\eta_2 - \eta_1)(z_1 + z_2)\\ &= \eta_2 z_2 - \eta_1 z_1 + \eta_2 z_1 - \eta_1 z_2 = \eta_2 z_2 - \eta_1 z_1 + \frac{\pi i}{2},\end{aligned}$$

et la formule précédente devient

$$\frac{e_3 - e_2}{e_3 - e_1} = -e^{2(\eta_2 z_2 - \eta_1 z_1)} \frac{\sigma^4 z_1}{\sigma^4 z_2}.$$

D'autre part [formule (7) (n° 134)]

$$\sigma_{10} = -e^{-\frac{\eta_1 z_1}{2}} \sigma z_1, \qquad \sigma_{01} = -e^{-\frac{\eta_2 z_2}{2}} \sigma z_2,$$

d'où

$$\lambda = -e^{2(\eta_2 z_2 - \eta_1 z_1)} \frac{\sigma^4 z_1}{\sigma^4 z_2}$$

et enfin

$$\lambda = \frac{e_3 - e_1}{e_3 - e_2}.$$

Rappelons que e_1, e_2, e_3, ∞ sont les quatre racines de la forme biquadratique fondamentale des fonctions elliptiques, réduite à la forme de Weierstrass

$$x_2(4x_1^3 - g_2 x_1^2 x_2 - g_3 x_2^3);$$

on peut dire que la fonction λ est le rapport anharmonique des points ayant pour abscisses ces quatre racines, prises dans un ordre convenable.

Il résulte de là :

1° Que les six valeurs de λ nous donnent les six valeurs du rapport anharmonique des quatre points pris dans toutes les dispositions possibles (on le voit d'ailleurs directement sur les expressions déjà trouvées des six rapports);

2° Que, à cause de la propriété invariante du rapport anharmonique, λ exprime le rapport anharmonique des racines de la forme biquadratique, qu'elle soit ou non réduite à la forme de Weierstrass.

En suivant la même marche que précédemment, mais avec des calculs toujours de plus en plus compliqués, on pourrait obtenir à l'aide de z les expressions des fonctions invariantes respectivement dans les sous-groupes Γ_{12}, Γ_{24}, Γ_{60}, fonctions dont nous pouvons *a priori* affirmer l'existence, en vertu du théorème du n° **132**.

Équations polyédriques et modulaires [1].

140. En égalant à une constante une quelconque des fonctions polyédriques ou modulaires, on obtient ce qu'on appelle une *équation polyédrique* ou une *équation modulaire*.

Ces équations peuvent être résolues par une méthode unique, fondée sur la considération d'une équation différentielle, dite *équation de* Schwarz.

Soit en général $Z(z)$ une fonction uniforme de z, prenant les mêmes valeurs en tous les points homologues d'un réseau régulier ayant pour angles $\frac{\pi}{\nu_1}, \frac{\pi}{\nu_2}, \frac{\pi}{\nu_3}$.

z peut être considérée comme une fonction de Z qui, pour chaque valeur de Z, prend plusieurs valeurs liées entre elles par des substitutions linéaires. Soient pour un instant pour z, ζ deux valeurs de z, correspondant à une même valeur de Z, de sorte que

$$\zeta = \frac{\alpha z + \beta}{\gamma z + \delta}, \tag{1}$$

ou bien

$$\gamma z\zeta + \delta\zeta - \alpha z - \beta.$$

Dérivant successivement trois fois par rapport à z, et désignant les dérivées par des accents, on obtient

$$\gamma(z\zeta' + z'\zeta) + \delta\zeta' - \alpha z' = 0,$$
$$\gamma(z\zeta'' + 2z'\zeta' + z''\zeta) + \delta\zeta'' - \alpha z'' = 0,$$
$$\gamma(z\zeta''' + 3z'\zeta'' + 3z''\zeta' + z'''\zeta) + \delta\zeta''' - \alpha z''' = 0,$$

[1] Dans la théorie des fonctions elliptiques, l'expression *équation modulaire* est prise dans un tout autre sens; c'est la relation entre les modules de deux fonctions elliptiques liées par une transformation de degré supérieur au premier. M. Klein distingue ces deux espèces d'équations en leur donnant les dénominations de *Modulgleichung* et *Modulargleichung*. Pour nous, il n'y a pas de confusion possible puisque nous n'étudions que les équations modulaires au sens précis indiqué dans le texte.

d'où, en éliminant α, γ, δ,

$$o = \begin{vmatrix} z' & \zeta' & z\zeta' + z'\zeta \\ z'' & \zeta'' & z\zeta'' + 2z'\zeta' + z''\zeta \\ z''' & \zeta''' & z\zeta''' + 3z'\zeta'' + 3z''\zeta' + z'''\zeta \end{vmatrix} = \begin{vmatrix} z' & \zeta' & o \\ z'' & \zeta'' & 2z'\zeta' \\ z''' & \zeta''' & 3(z'\zeta'' + z''\zeta') \end{vmatrix},$$

et, en développant,

$$\frac{\zeta'''}{\zeta'} - \frac{3}{2}\left(\frac{\zeta''}{\zeta'}\right)^2 = \frac{z'''}{z'} - \frac{3}{2}\left(\frac{z''}{z'}\right)^2.$$

θ étant une fonction de Z, nous représenterons l'expression

$$\frac{\theta'''}{\theta'} - \frac{3}{2}\left(\frac{\theta''}{\theta'}\right)^2$$

par la notation

$$[\theta]_Z.$$

Alors la dernière relation trouvée peut s'écrire

(1) $$[\zeta]_Z = [z]_Z;$$

elle exprime que $[z]_Z$ est une fonction uniforme de Z.

Pour déterminer l'expression $[z]_Z$, observons que la formule (1) du n° 130 peut s'écrire

$$z - z_0 = k(Z - Z_0) + k_1(Z - Z_0)^2 + k_2(Z - Z_0)^3 + \ldots,$$

et que, d'après les formules (1), (2), (3), (4), (5) du même paragraphe, on a successivement :

Pour un point z_0, distinct d'un nœud,

$$z' = k, \qquad z'' = 2k_1, \qquad z''' = 6k_2,$$

d'où

$$[z]_Z = \frac{6(kk_2 - k_1^2)}{k^2};$$

Pour un nœud a :

$$z' = \frac{k}{\nu_1}(Z-1)^{\frac{1}{\nu_1}-1}, \qquad z'' = \frac{k(1-\nu_1)}{\nu_1^2}(Z-1)^{\frac{1}{\nu_1}-2},$$

$$z''' = \frac{k(1-\nu_1)(1-2\nu_1)}{\nu^3}(z-1)^{\frac{1}{\nu_1}-3},$$

d'où

(2) $$[z]_Z = \frac{\nu_1^2 - 1}{2\nu_1^2}(Z-1)^{2}.$$

Pour un nœud b ou c, par un calcul analogue, on a respectivement

$$[z]_Z = \frac{\nu_2^2 - 1}{2\nu_2^2} Z^{-2}, \tag{3}$$

$$[z]_Z = \frac{\nu_3^2 - 1}{2\nu_3^2} Z^{-2}. \tag{4}$$

Dans le cas où l'une des quantités ν, par exemple ν_2, serait infinie, en posant

$$\frac{k}{z-b} - l = \frac{-lz + (k+bl)}{z-b} = v,$$

on a

$$v = \operatorname{Log} Z,$$

d'où

$$v' = Z^{-1}, \qquad v'' = -Z^{-2}, \qquad v''' = 2Z^{-3},$$

et, par conséquent, en tenant compte de (1),

$$[z]_Z = [v]_Z = \frac{1}{2} Z^{-2},$$

qui se déduirait de la formule obtenue dans le cas général, en y faisant $\nu_2 = \infty$.

Donc $[z]_Z$ est une fonction uniforme de Z, qui admet $Z = \infty$ pour zéro d'ordre deux, et n'a d'autres points singuliers que les deux pôles d'ordre deux $z = 1$, $z = 0$. C'est donc une fonction rationnelle [1] de Z de la forme suivante

$$[z]_Z = \frac{\rho + \sigma Z + \tau Z^2}{Z^2(Z-1)^2}, \tag{5}$$

ρ, σ, τ étant trois constantes qu'il s'agit de déterminer. De (2) (3), (4) résulte

$$\lim_{Z=1} \{(Z-1)^2 [z]_Z\} = \frac{\nu_1^2 - 1}{2\nu_1^2},$$

$$\lim_{Z=0} \{Z^2 [z]_Z\} = \frac{\nu_2^2 - 1}{2\nu_2^2},$$

$$\lim_{Z=\infty} \{Z^2 [z]_Z\} = \frac{\nu_3^2 - 1}{2\nu_3^2},$$

---

[1] D'après les principes de la théorie générale des fonctions, $[z]_Z$ étant uniforme et ayant pour seules singularités des pôles est une fonction rationnelle; de plus, les pôles doivent être les zéros de son dénominateur. Comme l'infini est un zéro d'ordre 2, le degré du numérateur est inférieur de deux unités à celui du dénominateur, ce qui conduit à la formule (5).

et, d'après (5),

$$\frac{\nu_1^2-1}{2\nu_1^2}=\rho+\sigma+\tau,\qquad \frac{\nu_2^2-1}{2\nu_2^2}=\rho,\qquad \frac{\nu_3^2-1}{2\nu_3^2}=\tau,$$

d'où

$$\begin{aligned}\sigma &= \frac{\nu_1^2-1}{2\nu_1^2}-\frac{\nu_2^2-1}{2\nu_2^2}-\frac{\nu_3^2-1}{2\nu_3^2}\\ &= \frac{1}{2}\left(\frac{1}{\nu_2^2}+\frac{1}{\nu_3^2}-\frac{1}{\nu_1^2}-1\right).\end{aligned}$$

La fonction cherchée est donc

$$(6)\quad \begin{aligned}[z]_Z &= \frac{1}{2}\left(1-\frac{1}{\nu_1^2}\right)\frac{1}{Z^2(Z-1)^2}\\ &+\frac{1}{2}\left(\frac{1}{\nu_2^2}+\frac{1}{\nu_3^2}-\frac{1}{\nu_1^2}-1\right)\frac{1}{Z(Z-1)^2}+\frac{1}{2}\left(1-\frac{1}{\nu_3^2}\right)\frac{1}{(Z-1)^2}.\end{aligned}$$

On peut écrire aussi

$$(7)\quad \begin{aligned}[z]_Z &= \frac{1}{2}\left(1-\frac{1}{\nu_1^2}\right)\frac{1}{(Z-1)^2}+\frac{1}{2}\left(1-\frac{1}{\nu_2^2}\right)\frac{1}{Z^2}\\ &+\frac{1}{2}\left(\frac{1}{\nu_1^2}+\frac{1}{\nu_2^2}-\frac{1}{\nu_3^2}-1\right)\frac{1}{Z(Z-1)}.\end{aligned}$$

L'équation différentielle écrite sous l'une ou l'autre des deux formes (6) et (7) s'appelle *équation de* Schwarz.

141. L'intégration de l'équation de Schwarz peut se ramener à l'intégration d'une équation linéaire et homogène du second ordre.

Soient l'équation linéaire

$$(1)\qquad y''+py'+qy=0$$

et y_1, y_2 deux de ses intégrales linéairement indépendantes; alors

$$(2)\qquad \begin{cases} y_1''+py_1'+qy_1=0,\\ y_2''+py_2'+qy_2=0,\end{cases}$$

d'où il suit

$$(3)\qquad p=-\frac{y_1''y_2-y_1y_2''}{y_1'y_2-y_1y_2'},$$

et en posant

$$\frac{y_1}{y_2}=\eta,$$

on aura

$$\eta' = \frac{y'_1 y_2 - y_1 y'_2}{y_2^2},$$

$$\frac{\eta''}{\eta'} = \frac{y''_1 y_2 - y_1 y''_2}{y'_1 y_2 - y_1 y'_2} - 2\frac{y'_2}{y_2},$$

et, à cause de (3),

$$\frac{\eta''}{\eta'} = -p - 2\frac{y'_2}{y_2}.$$

Par une nouvelle dérivation, on a

$$\frac{\eta'''}{\eta'} - \frac{\eta''^2}{\eta'^2} = -p' - 2\frac{y''_2}{y_2} + 2\frac{y'^2_2}{y_2^2},$$

d'où

$$[\eta]z = -p' - 2\frac{y''_2}{y_2} + 2\frac{y'^2_2}{y_2^2} - \frac{1}{2}\left(-p - 2\frac{y'_2}{y_2}\right)^2$$
$$= -p' - \frac{1}{2}p^2 - 2\frac{y''_2}{y_2} - 2p\frac{y'_2}{y_2},$$

où, d'après la seconde équation (2),

$$[\eta]z = -p' - \frac{1}{2}p^2 + 2q = r.$$

Donc le rapport de deux intégrales d'une équation linéaire et homogène du second ordre satisfait à une équation de Schwarz bien déterminée.

Donnons-nous, au contraire, une équation de Schwarz

(4) $$[\eta]z = r.$$

Posons

(5) $$r = -p' - \frac{1}{2}p^2 + 2q,$$

où p et q sont deux fonctions inconnues; si l'on prend p arbitrairement, q sera bien déterminé et il en sera de même de l'équation du second ordre (1) correspondant à l'équation donnée (4).

De l'intégrale générale de (1)

$$y = C_1 y_1 + C_2 y_2$$

on déduit aussitôt l'intégrale générale de (4)

$$\eta = \frac{C_1 y_1 + C_2 y_2}{C_3 y_1 + C_4 y_2}.$$

Supposons au contraire qu'on connaisse l'intégrale η de (4). Posons

$$y_2' y_2 - y_1 y_2' = y_2^2 \eta' = v; \tag{6}$$

on a, d'après (3),

$$v' + pv = 0;$$

d'où, en intégrant et désignant par C une constante arbitraire,

$$v = Ce^{-\int p\,dZ}. \tag{7}$$

La relation (6) donne ensuite

$$y_2 = \sqrt{\frac{C}{\eta'}}\, e^{-\frac{1}{2}\int p\,dZ},$$

d'où enfin

$$y_1 = \eta \sqrt{\frac{C}{\eta'}}\, e^{-\frac{1}{2}\int p\,dZ}.$$

142. On pouvait prévoir qu'à une équation (4) donnée devaient correspondre une infinité d'équations (1); car, η étant donnée, il y a une infinité de couples de fonctions y_1, y_2 dont le rapport est égal à η. Si donc nous choisissons un de ces couples, nous aurons par là même défini l'équation du second ordre correspondante. C'est bien le cas actuel, puisque les formules (1) du n° **128** déterminent t_1, t_2 comme fonctions de Z (et d'une autre variable X).

Nous nous proposons de construire l'équation du second ordre, admettant comme intégrales t_1 et t_2.

Posons, pour simplifier,

$$F_i(z_1, z_2) = F_i, \qquad F_i(z, 1) = \Phi_i,$$

$$\frac{d\Phi_i}{dz} = \Phi_i', \qquad \frac{\eta}{\nu_i} = k_i;$$

nous aurons, en vertu des propriétés connues des fonctions homogènes,

$$F_i = z_2^{k_i}\Phi_i, \qquad \frac{\partial F_i}{\partial z_i} = z_2^{k_i-1}\Phi_i', \qquad k_i F_i = z_1\frac{\partial F_i}{\partial z_1} + z_2\frac{\partial F_i}{\partial z_2},$$

d'où

$$\Phi_i = \frac{1}{z_2^{k_i}} F_i = \frac{1}{k_i z_2^{k_i}}\left(z_1\frac{\partial F_i}{\partial z_1} + z_2\frac{\partial F_i}{\partial z_2}\right),$$

$$\Phi_i' = \frac{1}{z_2^{k_i-1}}\frac{\partial F_i}{\partial z_i}.$$

Cela posé, dérivons par rapport à z la relation

$$Z = c\frac{F_2^{\nu_2}}{F_3^{\nu_3}} = c\frac{\Phi_2^{\nu_2}}{\Phi_3^{\nu_3}},$$

nous aurons

$$\begin{aligned} 1 &= c\frac{\Phi_2^{\nu_2-1}}{\Phi_3^{\nu_3+1}}(\nu_2\Phi_3\Phi'_2 - \nu_3\Phi_2\Phi'_3)\frac{dz}{dZ} \\ &= c\frac{\Phi_2^{\nu_2-1}}{\Phi_3^{\nu_3+1}}\,\frac{1}{z_2^{k_2+k_3-1}}\left[\frac{\nu_2}{k_3}\frac{\partial F_2}{\partial z_1}\left(z_1\frac{\partial F_3}{\partial z_1} + z_2\frac{\partial F_3}{\partial z_2}\right)\right. \\ &\qquad\left. - \frac{\nu_3}{k_2}\frac{\partial F_3}{\partial z_1}\left(z_1\frac{\partial F_2}{\partial z_1} + z_2\frac{\partial F_2}{\partial z_2}\right)\right]\frac{dz}{dZ}. \end{aligned}$$

Or

$$\frac{\nu_2}{k_3} = \frac{\nu_3}{k_2},$$

et (théorème d'Euler sur les polyèdres n° 52)

$$k_1 + 2 = k_2 + k_3,$$

d'où, c désignant une nouvelle constante,

$$1 = c\frac{\Phi_2^{\nu_2-1}}{\Phi_3^{\nu_3+1}}\,\frac{1}{z_2^{k_1}}\left(\frac{\partial F_2}{\partial z_1}\frac{\partial F_3}{\partial z_2} - \frac{\partial F_3}{\partial z_1}\frac{\partial F_2}{\partial z_2}\right)\frac{dz}{dZ}.$$

Mais (n° 123) F_1 étant, à un facteur constant près, le déterminant fonctionnel de F_2, F_3 ; en désignant par h, k deux constantes, on aura successivement

$$1 = h\frac{\Phi_2^{\nu_2-1}}{\Phi_3^{\nu_3-1}}\,\frac{1}{z_2^{k_1}}F_1\frac{dz}{dZ} = h\frac{\Phi_2^{\nu_2}}{\Phi_3^{\nu_3}}\,\frac{\Phi_1}{\Phi_2\Phi_3}\,\frac{dz}{dZ} = \frac{lZ}{X(z,1)}\,\frac{dz}{dZ} = \frac{lz_2^2 Z}{X}\,\frac{dz}{dZ},$$

$$\frac{dz}{dZ} = \frac{X}{lz_2^2 Z};$$

c'est-à-dire (en considérant comme au n° 128 les z_1, z_2 comme fonctions de Z et de X)

$$z_2\frac{dz_1}{dX} - z_1\frac{dz_2}{dX} = \frac{X}{lZ},$$

ou bien, à cause de (7) (n° 141),

$$\frac{X}{lZ} = Ce^{-\int p\,dz}$$

On tire de là

$$\int p\, dZ = \operatorname{Log} Z + \operatorname{Log} \frac{Cl}{X},$$

et dérivant par rapport à z

$$p = \frac{1}{Z}.$$

p une fois connue, r et q sont données respectivement par le second membre de (6) (n° **140**) et la formule (5) (n° **141**).

L'équation différentielle à laquelle satisfont z_1 et z_2 est donc

$$0 = y'' + \frac{1}{Z} y' + \frac{1}{4Z^2(Z-1)^2}\left[-\frac{1}{\nu_1^2} + \left(\frac{1}{\nu_2^2} + \frac{1}{\nu_3^2} - \frac{1}{\nu_1^2} + 1\right)Z - \frac{1}{\nu_3^2} Z^2\right] y.$$

Elle appartient à la classe bien connue des *équations de* RIEMANN

$$(1) \quad P'' + \frac{1}{Z(1-Z)}(A + BZ)P' + \frac{1}{Z^2(1-Z)^2}(C + DZ + EZ^2)P = 0.$$

On désigne habituellement l'intégrale de (1) par la notation

$$P\begin{pmatrix} \alpha, & \beta, & \gamma, & \\ \alpha', & \beta', & \gamma', & Z \end{pmatrix},$$

$\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ étant six constantes satisfaisant à la condition

$$\alpha + \alpha' + \beta + \beta' + \gamma + \gamma' = 1,$$

et liées à A, B, C, D, E par les relations

$$A = 1 - \alpha - \alpha', \qquad B = -1 - \beta - \beta', \qquad C = \alpha\alpha',$$
$$D = -\alpha\alpha' - \beta\beta' + \gamma\gamma', \qquad E = \beta\beta'.$$

Si l'on pose

$$P = Z^{\alpha}(1-Z)^{\gamma}\varphi, \qquad a = \alpha + \beta + \gamma,$$
$$b = \beta' + \gamma + \alpha, \qquad c = 1 + \alpha - \alpha',$$

l'équation (1) devient

$$(2) \qquad Z(1-Z)\varphi'' + [c - (a + b + 1)Z]\varphi' - ab\varphi = 0.$$

C'est une *équation hypergéométrique* ou *équation de* GAUSS. Il est facile de vérifier directement que cette équation est satis-

faite par la série *hypergéométrique*

$$(3)\quad \left\{ \begin{aligned} \varphi = F(a, b, c, Z) &= 1 + \frac{ab}{1c} Z + \frac{a(a+1)b(b+1)}{1.2c(c+1)} Z^2 \\ &+ \frac{a(a+1)(a+2)b(b+1)(\beta+2)}{1.2.3c(c+1)(c+2)} Z^3 + \ldots \end{aligned} \right.$$

Si l'on pose

$$\varphi = Z^{1-c}\psi, \qquad a' = a + 1 - c, \qquad b' = b + 1 - c, \qquad c' = 2 - c,$$

l'équation (2) se transforme en une équation du même type

$$Z(Z-1)\psi'' + [c' - (a' + b' + 1)Z]\psi' - a'b'\psi = 0,$$

qui admet l'intégrale

$$\psi = F(a', b', c', Z).$$

Il en résulte que (2) admet l'intégrale

$$(4)\qquad \varphi = Z^{1-c} F(a', b', c', Z).$$

Aux intégrales (3) et (4) de (2) correspondent les deux intégrales suivantes de (1) :

$$\begin{aligned} P &= Z^{\alpha}(1-Z)^{\gamma} F(a, b, c, Z), \\ P &= Z^{\alpha+1-c}(1-Z)^{\gamma} F(a', b', c', Z) \\ &= Z^{\alpha'}(1-Z)^{\gamma} F(a', b', c', Z). \end{aligned}$$

143. Dans le cas actuel, on a

$$A = 1, \qquad B = -1, \qquad C = -\frac{1}{4\nu_2^2},$$

$$D = \frac{1}{4}\left(\frac{1}{\nu_2^2} + \frac{1}{\nu_3^2} - \frac{1}{\nu_1^2} + 1\right), \qquad E = -\frac{1}{4\nu_3^2},$$

d'où

$$\alpha + \alpha' = 0, \qquad \beta + \beta' = 0, \qquad \gamma + \gamma' = 1,$$

$$\alpha\alpha' = -\frac{1}{4\nu_2^2}, \qquad \beta\beta' = -\frac{1}{4\nu_3^2}, \qquad \gamma\gamma' = \frac{1}{4}\left(1 - \frac{1}{\nu_1^2}\right)$$

et, par suite,

$$\alpha = \frac{1}{2\nu_2}, \qquad \alpha' = -\frac{1}{2\nu_2}, \qquad \beta = \frac{1}{2\nu_3}, \qquad \beta' = -\frac{1}{2\nu_3},$$

$$\gamma = \frac{1}{2}\left(1 + \frac{1}{\nu_1}\right), \qquad \gamma' = \frac{1}{2}\left(1 - \frac{1}{\nu_1}\right)$$

et

$$a = \frac{1}{2}\left(1 + \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3}\right),$$

$$b = \frac{1}{2}\left(1 + \frac{1}{\nu_1} + \frac{1}{\nu_2} - \frac{1}{\nu_3}\right), \qquad c = 1 + \frac{1}{\nu_2},$$

$$a' = \frac{1}{2}\left(1 + \frac{1}{\nu_1} - \frac{1}{\nu_2} + \frac{1}{\nu_3}\right),$$

$$b' = \frac{1}{2}\left(1 + \frac{1}{\nu_1} - \frac{1}{\nu_2} - \frac{1}{\nu_3}\right), \qquad c' = 1 - \frac{1}{\nu_2}.$$

Les deux intégrales trouvées prennent donc la forme

$$(1) \quad \begin{cases} P = Z^{-\frac{1}{2\nu_2}}(1 - Z)^{\frac{1}{2}\left(1 + \frac{1}{\nu_1}\right)} F(a', b', c', Z), \\ P = Z^{\frac{1}{2\nu_2}}\;(1 - Z)^{\frac{1}{2}\left(1 + \frac{1}{\nu_1}\right)} F(a, b, c, Z), \end{cases}$$

a, b, c, a', b', c' ayant les valeurs qu'on vient d'indiquer.

A l'aide de ces deux intégrales, on pourra exprimer sans difficulté les deux intégrales cherchées z_1, z_2; le rapport $z = \frac{z_1}{z_2}$ donnera z en fonction de Z et permettra de résoudre l'équation polyédrique ou modulaire.

Pour faciliter cette résolution, modifions l'orientation des polyèdres de façon que le pôle d'une face coïncide avec le point de la sphère correspondant au point $z = 0$ du plan. Alors, pour $z = 0$, on a $Z = 0$, d'où (n° 130), k désignant une constante différente de zéro,

$$z = kZ^{\frac{1}{\nu_2}} + \ldots.$$

D'autre part, F_3, s'annulant aux pôles des faces, doit contenir, une fois et une fois seulement, le facteur z, tandis que ce facteur ne figure ni dans F_1, ni dans F_3; alors dans le domaine de l'origine, on a

$$X(z, 1) = hz + \ldots,$$

h désignant une constante différente de zéro, et par suite

$$z_1 = z\frac{\sqrt{X}}{\sqrt{X(z, 1)}} = \frac{\sqrt{X}}{\sqrt{h}} z^{\frac{1}{2}} + \ldots,$$

$$z_2 = \frac{\sqrt{X}}{\sqrt{h}} z^{-\frac{1}{2}} + \ldots,$$

ou bien, en désignant par λ_1, λ_2 deux constantes non nulles,

$$z_1 = \lambda_1 Z^{\frac{1}{2\nu_2}} + \ldots,$$
$$z_2 = \lambda_2 Z^{-\frac{1}{2\nu_2}} + \ldots.$$

Donc, dans le cas considéré, les deux intégrales cherchées ne sont autres, à des facteurs constants près, que les intégrales (1).

144. Au lieu d'exprimer directement les irrationnelles polyédriques et modulaires ([1]) par un développement en séries hypergéométriques de Z, on peut en se bornant à l'équation modulaire employer la méthode qu'on vient d'exposer. On cherchera ensuite à exprimer l'irrationalité diédrique pour $m = 3$, et les irrationalités tétraédrique, octaédrique et icosaédrique en fonction uniforme de l'irrationalité modulaire, ce qui est possible en vertu du théorème du n° **131**. La construction effective de telles fonctions se confond avec celles des fonctions invariantes dans les sous-groupes Γ_6, Γ_{12}, Γ_{24}, Γ_{60} de Γ, problème dont nous nous sommes occupé précédemment.

Pour l'irrationalité modulaire, on a

$$\nu_1 = 2, \qquad \nu_2 = 3, \qquad \nu_3 = \infty,$$

d'où

$$a = b = \frac{11}{12}, \qquad c = \frac{4}{3}, \qquad a' = b' = \frac{7}{12}, \qquad c' = \frac{2}{3},$$

et les formules (1) (n° **143**) donnent, à un facteur constant près facile à déterminer,

$$(1) \qquad z = Z^{\frac{1}{3}} \frac{F\left(\frac{11}{12}, \frac{11}{12}, \frac{4}{3}, Z\right)}{F\left(\frac{7}{12}, \frac{7}{12}, \frac{2}{3}, Z\right)}.$$

Or, nous avons trouvé (n° **139**)

$$\lambda = -\frac{\sigma_{10}^4}{\sigma_{01}^4}.$$

([1]) Nous appelons pour abréger *irrationalité polyédrique* ou *modulaire* la fonction z de Z définie par $Z = F(z)$, F étant une équation polyédrique ou modulaire.

Remplaçons dans le second membre z par l'expression (1), λ sera exprimée en fonction de Z, ce qui nous permettra de résoudre l'équation diédrique dans le cas de $m = 3$.

On parviendrait, d'une façon analogue, à la résolution des autres équations polyédriques.

Étude algébrique des équations polyédriques et de l'équation modulaire. Résolvantes.

145. Avant d'étudier les équations polyédriques au point de vue exclusivement algébrique, il convient de rappeler certaines propositions dont nous ferons usage dans la suite.

Étant donnée une fonction rationnelle f de plusieurs variables x_1, x_2, ..., x_n, on appelle *groupe appartenant à la fonction* f le groupe des permutations des variables, qui laissent cette fonction invariable; on dit aussi que la fonction *appartient* au groupe considéré.

Si f est une fonction symétrique, le groupe correspondant appelé groupe *symétrique* comprend toutes les permutations en nombre $n!$ des variables $x_1, x_2, \ldots, x_n$.

Si, pour toutes les permutations possibles, une fonction f ne prend que deux valeurs, le groupe appartenant à cette fonction est formé des $\frac{1}{2}n!$ permutations paires; on l'appelle groupe *alterné*. Tel serait, par exemple, le déterminant de Vandermonde qui, par l'effet d'une permutation quelconque, reste invariable, ou bien change de signe.

Soit Δ le discriminant des n variables, c'est-à-dire le produit des carrés de leurs $\frac{n(n-1)}{2}$ différences. Toute fonction appartenant au groupe alterné est de la forme

$$\varphi + \psi\sqrt{\Delta},$$

où φ et ψ sont des fonctions symétriques; pour toutes les permutations des variables cette fonction est susceptible des deux formes suivantes :

$$\varphi + \psi\sqrt{\Delta}, \qquad \varphi - \psi\sqrt{\Delta}.$$

Si, pour toutes les permutations des variables, une fonction f est susceptible de s formes diverses

$$f, \ f_1, \ f_2, \ \ldots, \ f_{s-1},$$

le nombre s est le quotient de $n\,!$ par l'ordre du groupe, c'est-à-dire l'indice de groupe de la fonction, considéré comme sous-groupe du groupe symétrique. Les groupes des fonctions f, f_1, f_2, ..., f_{s-1} sont autant de sous-groupes du groupe symétrique, équivalents au groupe de f et non nécessairement distincts.

Soient G, H les groupes des fonctions f, φ; si H est un sous-groupe de G, f peut s'exprimer rationnellement à l'aide de φ et des fonctions symétriques, et réciproquement.

En particulier, quand deux fonctions f et φ ont le même groupe, elles peuvent s'exprimer rationnellement l'une par l'autre, les coefficients étant des fonctions symétriques.

Étant donnée une équation algébrique, ses coefficients nous donnent les valeurs des fonctions symétriques des racines. Il peut arriver qu'on connaisse en même temps la valeur de quelque fonction φ des racines non symétrique. Si G est le groupe de φ, on connaîtra en même temps que φ la valeur de toute autre fonction du groupe G, puisqu'une telle fonction est exprimable rationnellement à l'aide de φ et des coefficients de l'équation.

Si l'on connaissait les valeurs de plusieurs fonctions φ, ψ, χ, appartenant à différents groupes G, H, K, ..., on connaîtrait aussi la valeur de la fonction

$$F = \alpha\varphi + \beta\psi + \gamma\chi + \ldots,$$

α, β, γ, ... étant des nombres quelconques distincts ou encore des quantités indéterminées. Le groupe de F est le plus grand sous-groupe commun à G, H, K, puisque la condition nécessaire pour que F reste invariable est qu'il en soit de même de chacune des fonctions φ, ψ, χ, ... On voit donc qu'on peut toujours se borner au cas où l'on connaît la valeur *d'une* fonction (et avec elle naturellement celle de toutes les autres fonctions appartenant au même groupe). Le groupe auquel appartient cette fonction s'appelle le *groupe de l'équation*.

Pour une équation *générale*, c'est-à-dire où les seules fonctions

rationnelles connues des racines sont les fonctions symétriques, le groupe est le groupe symétrique.

Si, au contraire, on connaît par exemple la valeur de la racine carrée du discriminant, le groupe de l'équation est le groupe alterné.

Lorsqu'une équation est irréductible, son groupe est transitif (n° 15) et réciproquement.

Soient $f(z) = 0$ une équation de degré n, dont les coefficients appartiennent à un certain domaine de rationalité ([1]) C, y une fonction rationnelle des racines z, z_1, z_2, ..., z_{n-1}, et dont les coefficients appartiennent au même domaine. Si, par l'effet des r permutations des racines, r désignant l'ordre du groupe G de l'équation, la fonction y prend s valeurs diverses

$$y, \quad y_1, \quad y_2, \quad \ldots, \quad y_{s-1},$$

les fonctions symétriques de ces s valeurs appartiendront au domaine C.

En effet, ce sont des fonctions symétriques des racines de l'équation donnée, dont les coefficients appartiennent à C. Ainsi $y, y_1, y_2, \ldots, y_{s-1}$ seront les racines d'une équation de degré s, dont les coefficients appartiendront au domaine C. Cette équation, que nous écrirons

$$\varphi(y) = 0, \tag{1}$$

est dite une *résolvante* de l'équation donnée. Le groupe G de l'équation proposée et le groupe H de la résolvante sont isomorphes ([2]); l'isomorphisme peut être holoédrique ou mériédrique; il est nécessairement holoédrique si G est un groupe simple.

Si l'isomorphisme est holoédrique, à chaque permutation des z autre que l'identité correspond une permutation des y autre que l'identité et *vice versa*. Donc, il n'y a que la permutation iden-

---

([1]) On appelle *domaine de rationalité* $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ l'ensemble des fonctions rationnelles de $\alpha_1, \alpha_2, \ldots, \alpha_n$. Ainsi, par exemple, le domaine de rationalité [1] est constitué par l'ensemble de tous les nombres rationnels.

([2]) En effet à chaque permutation des z correspond une permutation déterminée des y; d'autre part au produit de deux permutations des z correspond le produit des deux permutations des y.

tique des z qui laisse tous les y invariables. Il suit de là que le groupe de la fonction

$$\eta = \alpha y + \alpha_1 y_2 + \ldots + \alpha_{s-1} y_{s-1}, \tag{2}$$

où les α sont des constantes distinctes, comprend seulement l'identité, que les z s'expriment rationnellement à l'aide de η et des quantités du domaine C, et que, par suite, l'équation proposée peut être regardée comme une résolvante de (1). On dit alors que (1) est une *résolvante équivalente*, puisque la résolution de l'équation $f(z) = 0$ et celle de $\varphi(y) = 0$ constituent des problèmes équivalents.

Si l'isomorphisme est mériédrique, à la permutation identique du groupe H correspond dans le groupe G un sous-groupe invariant G′ : c'est l'ensemble des permutations des z qui laissent invariable la fonction (2). Supposons qu'on sache résoudre l'équation (1) et qu'on connaisse par conséquent la valeur de la fonction η, le groupe de l'équation donnée n'est plus G, mais se réduit à G′ [1]. Donc, étant donnée une résolvante non équivalente, sa résolution réduit le groupe de l'équation à un sous-groupe invariant du même groupe.

Une résolvante équivalente particulièrement importante est la *résolvante de* Galois. On désigne ainsi l'équation irréductible dont l'une des racines est

$$\rho = \beta z + \beta_1 z_1 + \ldots + \beta_{n-1} z_{n-1},$$

$\beta, \beta_1, \beta_2, \ldots, \beta_{n-1}$ étant des constantes distinctes. Puisque chaque permutation des z change la valeur de ρ, le groupe de la fonction ρ comprend seulement l'identité, et tous les z peuvent s'exprimer rationnellement à l'aide de ρ. De plus, comme toutes les racines de cette résolvante se déduisent de ρ en échangeant les z entre eux, ces racines sont des fonctions appartenant au groupe formé de la seule identité, et peuvent donc s'exprimer rationnellement à l'aide d'une quelconque d'entre elles.

Soient $\rho, \rho_1, \rho_2, \ldots, \rho_{r-1}$ ces racines, on a

$$\rho_i = \psi_i(\rho) \qquad (i = 1, 2, \ldots, r-1),$$

---

[1] G′ est le sous-groupe commun au groupe de la fonction y et aux groupes qui lui sont équivalents.

les ψ_i étant des symboles de fonctions rationnelles. Chaque fonction ψ_i correspond à une permutation déterminée S_i du groupe G, celle qui change ρ en ρ_i; au produit des deux permutations S_i, S_h correspond la fonction $\psi_i\psi_h$. Donc les ψ_i, regardés comme symboles d'opérations, constituent un groupe Γ, holoédriquement isomorphe au groupe G.

Soit

$$F(u) = 0 \tag{3}$$

la résolvante de Galois. Appliquons-lui le changement de variables

$$v = \psi_h(u),$$

elle devient

$$F[\psi_h^{-1}(v)] = \Phi(v) = 0. \tag{4}$$

Les racines de (3) sont

$$u = \rho, \qquad u = \psi_1(\rho), \qquad \ldots, \qquad u = \psi_{r-1}(\rho).$$

Celles de (4) sont les expressions de v que l'on déduit des relations

$$\psi_h^{-1}(v) = \rho, \qquad \psi_h^{-1}(v) = \psi_1(\rho), \qquad \ldots, \qquad \psi_h^{-1}(v) = \psi_{r-1}(\rho),$$

c'est-à-dire

$$v = \psi_h(\rho), \qquad v = \psi_1\psi_h(\rho), \qquad \ldots, \qquad v = \psi_{r-1}\psi_h(\rho). \tag{5}$$

Mais puisque les opérations ψ forment un groupe, les opérations (5) ne sont autres que ψ, ψ_1, ψ_2, ..., ψ_r rangées dans un certain ordre. Donc les équations (3) et (4) ont les mêmes racines et par suite chacune des fonctions ψ transforme en elle-même la résolvante de Galois. Cette résolvante jouit donc de la propriété d'admettre des transformations rationnelles en elle-même, et le nombre de ces transformations est égal à son degré.

Réciproquement si une équation irréductible de degré r

$$F(u) = 0$$

admet r transformations rationnelles en elle-même

$$v = u, \qquad v = \psi_1(u), \qquad v = \psi_2(u), \qquad \ldots, \qquad v = \psi_{r-1}(u),$$

on a, en désignant par h l'un quelconque des nombres 1, 2, ..., $r-1$,

$$F(u) = F[\psi_h^{-1}(u)] \quad (^1).$$

On voit que si ρ est une racine de l'équation donnée, il en est de même de la quantité u donnée par

$$\psi_h^{-1}(u) = \rho,$$

c'est-à-dire de

$$u = \psi_h(\rho).$$

Donc les racines de l'équation sont toutes des fonctions rationnelles de l'une d'entre elles, et l'équation peut être regardée comme sa propre résolvante de GALOIS. En outre, le groupe formé des opérations ψ est holoédriquement isomorphe au groupe de l'équation, et peut être pris évidemment pour groupe de l'équation.

146. Appliquons les considérations précédentes aux équations polyédriques.

Soient

$$Z(z) = Z$$

une équation polyédrique (ou cyclique), G le groupe correspondant, n l'ordre de ce groupe. Si l'on soumet l'équation aux n substitutions linéaires de G, l'équation ne change pas, en sorte que G peut être considéré comme le groupe de cette équation. De plus G est transitif, car, si l'on prend deux points homologues quelconques, il existe toujours dans G une substitution qui échange ces deux points. L'équation est par suite irréductible. Donc :

Toute équation polyédrique est irréductible; son groupe est le groupe polyédrique correspondant, et elle peut être considérée comme sa propre résolvante de GALOIS.

147. *a.* La résolution des équations cycliques est du domaine de l'Algèbre élémentaire.

---

(1) Les deux membres pourraient aussi différer par un facteur constant, cela n'a pour nous aucune importance.

En effet, l'équation

(1) $$Z^n = Z$$

se résout au moyen d'une simple extraction de racine

$$z = \sqrt[n]{Z}.$$

b. De même les équations diédriques

(2) $$\frac{(z^m + 1)^2}{4z^m} = Z$$

sont des équations élémentaires ; elles appartiennent à la classe des équations qui se ramènent au second degré. Nous pouvons, cependant, leur appliquer les théories générales précédentes.

Puisque le groupe diédrique d'ordre $n = 2m$ contient un sous-groupe cyclique invariant d'ordre m, nous prendrons comme résolvante (non équivalente) de (2) une équation ayant pour racine une fonction appartenant à ce sous-groupe, par exemple la fonction $z^m = Z_1$. Cette équation

$$\frac{(Z_1 + 1)^2}{4Z_1} = Z$$

se réduit par voie élémentaire à l'équation cyclique du deuxième ordre

$$(Z_1 - 2Z + 1)^2 = 4Z(Z - 1),$$

d'où

$$Z_1 = 2Z - 1 + 2\sqrt{Z(Z-1)}$$

et enfin

$$z = \sqrt[m]{2Z - 1 + 2\sqrt{Z(Z-1)}}.$$

En particulier pour le groupe trirectangle ($m = 2$)

(3) $$z = \sqrt{2Z - 1 + 2\sqrt{Z(Z-1)}} = \sqrt{Z} + \sqrt{Z-1}.$$

c. Le groupe tétraédrique admet comme sous-groupe invariant un groupe trirectangle. Or l'équation tétraédrique

$$\frac{\varphi^3}{\psi^3} = \left(\frac{z^4 + 2i\sqrt{3}z^2 + 1}{z^4 - 2i\sqrt{3}z^2 + 1}\right)^3 = Z$$

peut s'écrire, en posant $\alpha = e^{\frac{2\pi i}{3}}$,

$$\left[\frac{(z^2+1)^2+4\alpha z^2}{(z^2+1)^2+4\alpha^2 z^2}\right]^3 = Z,$$

ou encore

$$(4)\qquad \left[\frac{\dfrac{(z^2+1)^2}{4z^2}+\alpha}{\dfrac{(z^2+1)^2}{4z^2}+\alpha^2}\right]^3 = Z.$$

Prenons pour résolvante une équation ayant pour racine une fonction invariante dans le groupe trirectangle, par exemple la fonction

$$\frac{(z^2+1)^2}{4z^2} = Z_1.$$

L'équation cherchée, qu'on déduit aussitôt de (4), est

$$\left(\frac{Z_1+\alpha}{Z_1+\alpha^2}\right)^3 = Z.$$

C'est une équation cyclique, d'où l'on tire

$$(5)\qquad Z_1 = -\frac{\alpha^2\sqrt[3]{Z}-\alpha}{\sqrt[3]{Z}-1},$$

et, en tenant compte de (3),

$$(6)\qquad z = \sqrt{Z_1}+\sqrt{Z_1-1},$$

Z_1 étant donné par la relation (5).

d. Le groupe octaédrique contient comme sous-groupe invariant un groupe tétraédrique.

Or, l'équation octaédrique

$$\frac{W^3}{108t^4} = Z,$$

en vertu des relations (n° 125 et n° 126)

$$W = \varphi\psi, \qquad 12i\sqrt{3}t^2 - \varphi^3 + \psi^3 = 0,$$

peut s'écrire

$$(7)\qquad \frac{-4\left(\dfrac{\varphi}{\psi}\right)^3}{\left[\left(\dfrac{\varphi}{\psi}\right)^3-1\right]^2} = Z.$$

Prenons comme résolvante une équation dont l'une des racines

soit une fonction invariante dans le groupe tétraédrique, par exemple la fonction

$$\left(\frac{\varphi}{\psi}\right)^3 = Z_2.$$

Une telle équation, qu'on déduit aussitôt de (7),

$$\frac{-4Z_2}{(Z_2-1)^2} = Z,$$

se réduit à une équation cyclique qui, résolue, donne

(8) $$Z_2 = \frac{Z-2+2\sqrt{1-Z}}{Z}.$$

On a donc, en se reportant à la relation (6),

$$Z = \sqrt{Z_3} + \sqrt{Z_3 - 1},$$

Z_3 ayant pour valeur d'après (5)

$$Z_3 = -\frac{\alpha^2\sqrt[3]{Z_2} - \alpha}{\sqrt[3]{Z_2} - 1}.$$

Quant à Z_2, elle est définie par (8).

148. Rien de ce qui vient d'être dit ne subsiste pour le groupe icosaédrique, qui, étant un groupe simple, ne peut donner lieu à des résolvantes non équivalentes. Construisons cependant une résolvante qui présentera pour nous un intérêt spécial.

Le groupe icosaédrique contient cinq sous-groupes tétraédriques équivalents. Or, si nous construisons une fonction invariable par les substitutions d'un de ces groupes; cette fonction, pour toutes les substitutions du groupe icosaédrique, prendra cinq valeurs distinctes. Ces cinq valeurs seront racines d'une équation du cinquième degré, qui sera une résolvante de l'équation icosaédrique. La fonction considérée est rationnelle en z et du douzième degré.

Choisissons, pour fixer les idées, le sous-groupe tétraédrique correspondant au système des trois médianes orthogonales, passant par le milieu de l'arête 1-2 et que nous avons désigné (n° 67) par la notation k_1. Soit t' la forme du sixième degré qui s'annule aux extrémités de ces trois médianes, la fonction

(1) $$r = \frac{t'^2}{f}$$

sera une fonction du douzième degré invariante dans le sous-groupe tétraédrique considéré.

La forme t' est celle que nous avions déjà représentée par t, dans une autre position du tétraèdre. Elle se déduit d'ailleurs de t par la substitution linéaire représentative de la rotation, amenant les trois médianes d'un même système en coïncidence avec les trois axes de coordonnées.

Cette rotation, comme il est facile de le voir, a pour amplitude $\frac{l}{2}$ et s'effectue autour de l'axe η. On doit donc, dans les formules (6) du n° 61, poser

$$\beta = \frac{l}{4}, \qquad \lambda = 0, \qquad \mu = 90,$$

d'où

$$a = c = 0, \qquad b = -\sin\frac{l}{4}, \qquad d = \cos\frac{l}{4},$$

et la formule (3) du même paragraphe devient

$$z' = \frac{z\cos\frac{l}{4} + \sin\frac{l}{4}}{-z\sin\frac{l}{4} + \cos\frac{l}{4}},$$

ou bien, sous forme homogène unitaire,

$$z'_1 = z_1\cos\frac{l}{4} + z_2\sin\frac{l}{4}, \qquad z'_2 = -z_1\sin\frac{l}{4} + z_2\cos\frac{l}{4};$$

on a ensuite

$$\begin{aligned}
t' &= z'_1 z'_2(z'^4_1 - z'^4_2)\\
&= \left[-(z_1^2 - z_2^2)\cos\frac{l}{4}\sin\frac{l}{4} + z_1 z_2\left(\cos^2\frac{l}{4} - \sin^2\frac{l}{4}\right)\right]\\
&\quad\times\left[(z_1^4 - z_2^4)\left(\cos^2\frac{l}{4} - \sin^2\frac{l}{4}\right) + 4z_1 z_2(z_1^2 + z_2^2)\sin\frac{l}{4}\cos\frac{l}{4}\right]\\
&= \frac{1}{2}\left[-(z_1^2 - z_2^2)\sin\frac{l}{2} + 2z_1 z_2\cos\frac{l}{2}\right]\\
&\quad\times\left[(z_1^2 - z_2^2)\cos\frac{l}{2} + 2z_1 z_2\sin\frac{l}{2}\right](z_1^2 + z_2^2)\\
&= \frac{1}{2}(z_1^2 + z_2^2)\left[-\frac{1}{2}(z_1^4 + z_2^4 - 6z_1^2 z_2^2)\sin l + 2z_1 z_2(z_1^2 - z_2^2)\cos l\right].
\end{aligned}$$

Or (n° 65)

$$\sin l = \frac{2}{\sqrt{5}}, \qquad \cos l = \frac{1}{\sqrt{5}},$$

d'où

$$t' = -\frac{1}{2\sqrt{5}}(z_1^2 + z_2^2)(z_1^4 - 2z_1^3 z_2 - 6z_1^2 z_2^2 + 2z_1 z_2^3 + z_2^4)$$

ou bien, en supprimant le facteur $-\frac{1}{2\sqrt{5}}$,

$$t' = z_1^6 - 3z_1^5 z_2 - 5z_1^4 z_2^2 - 5z_1^2 z_2^4 + 2z_1 z_2^5 + z_2^6.$$

Notre fonction est donc

$$r = \frac{(z_1^6 - 2z_1^5 z_2 - 5z_1^4 z_2^2 - 5z_1^2 z_2^4 + 2z_1 z_2^5 + z_2^6)^2}{z_1 z_2(z_1^{10} - 11z_1^5 z_2^5 - z_2^{10})},$$

ou encore

$$r = -\frac{(z^6 - 2z^5 - 5z^4 - 5z^2 + 2z + 1)^2}{z(z^{10} - 11z^5 - 1)}.$$

L'équation du cinquième degré entre r et Z peut s'écrire

$$(2) \qquad \frac{Z - 1}{\varphi(r)} = \frac{Z}{\psi(r)} = \frac{1}{\chi(r)},$$

$\varphi(r)$, $\psi(r)$, $\chi(r)$ étant trois polynomes de degré au plus égal à 5, dont l'un au moins est du cinquième degré, et dont les racines sont les valeurs que prend r respectivement au milieu des arêtes, aux centres des faces et aux sommets de l'icosaèdre. Ces trois polynomes sont liés par la relation

$$(3) \qquad \varphi(r) = \psi(r) - \chi(r).$$

Tout d'abord (1) montre que r est infini en tous les sommets; donc les racines de $\chi(r)$ doivent être toutes infinies, ce qui exige que $\chi(r)$ se réduise à une constante. Nous poserons

$$(4) \qquad \chi(r) = 1728.$$

Il résulte encore de (1) que r s'annule en 6 des milieux des 30 arêtes. Aux 24 autres points, r doit prendre 4 autres valeurs. Mais puisque les substitutions du groupe tétraédrique laissent la fonction r invariable (ainsi que le système k_1 de trois médianes), mais ne laissent invariable aucun autre système de trois médianes, la valeur que prend r aux extrémités de l'un des 4 systèmes k_2, k_3,

k_4, k_5 devra être égale à celle qu'elle prend aux extrémités d'un autre système. Autrement dit, les quatre valeurs devront être égales deux à deux. La fonction $\varphi(r)$ aura donc la forme suivante :

$$\varphi(r) = \mu r(r^2 + \alpha r + \beta)^2. \tag{5}$$

Quant aux centres des 20 faces de l'icosaèdre, 8 d'entre eux coïncident (n° 75) avec les centres des faces de l'octaèdre, ayant pour sommets les extrémités du système k_1, ou bien encore avec les sommets du cube polaire. Ces sommets, par les rotations du groupe tétraédrique se changent entre eux quatre à quatre (puisqu'ils forment deux tétraèdres polaires l'un de l'autre, dont chacun se change en lui-même); les 12 autres points, ne pouvant contenir aucun ensemble de 4 sommets, qui reste invariable, s'échangent tous entre eux. Et comme les centres des faces doivent être regardés comme des points triples, $\psi(r)$ aura deux racines simples et une racine triple, d'où

$$\psi(r) = \nu(r + \gamma)^3(r^2 + \delta r + \varepsilon). \tag{6}$$

Les coefficients figurant dans (5) et (6) se déterminent au moyen de (2), (3), (4). En vertu de ces relations, on a

$$\mu r(r^2 + \alpha r + \beta)^2 = \nu(r + \gamma)^3(r^2 + \delta r + \varepsilon) - 1728, \tag{7}$$

$$Z = \frac{\nu(r + \gamma)^3(r^2 + \delta r + \varepsilon)}{1728}.$$

Or (n° 128)

$$Z = -\frac{H^3}{1728 f^5}.$$

Pour $z = \infty$, il résulte cette formule et de l'expression de r

$$r = z, \qquad Z = \frac{\nu r^5}{1728} = \frac{\nu z^5}{1728}, \qquad Z = \frac{z^5}{1728},$$

d'où

$$\nu = 1.$$

Ensuite la comparaison des termes de plus haut degré dans (7) donne

$$\mu = \nu,$$

d'où

$$\mu = \nu = 1$$

et

$$\varphi(r) = r(r^2 + \alpha r + \beta)^2, \qquad \psi(r) = (r + \gamma)^3(r^2 + \delta r + \varepsilon),$$

(7) devient donc

$$(8) \qquad r(r^2 + \alpha r + \beta)^2 = (r + \gamma)^3(r^2 + \delta r + \varepsilon) - 1728.$$

Dérivons les deux membres de cette identité, nous aurons

$$(r^2 + \alpha r + \beta)^2 + 2r(r^2 + \alpha r + \beta)(2r + \alpha)$$
$$= 3(r + \gamma)^2(r^2 + \delta r + \varepsilon) + (r + \gamma)^3(2r + \delta)$$

ou bien

$$(r^2 + \alpha r + \beta)(5r^2 + 3\alpha r + \beta)$$
$$= (r + \gamma)^2[5r^2 + (2\gamma + 4\delta)r + \gamma\delta + 3\varepsilon].$$

Le facteur $r + \gamma$ ne peut diviser le trinome $r^2 + \alpha r + s$, puisque les valeurs que prend r aux centres des faces sont nécessairement différentes de celles qu'il prend aux milieux des arêtes.

On doit donc avoir

$$5r^2 + 3\alpha r + \beta = 5(r + \gamma)^2,$$
$$5r^2 + (2\gamma + 4\delta)r + \gamma\delta + 3\varepsilon = 5(r^2 + \alpha r + \beta),$$

d'où

$$3\alpha = 10\gamma, \qquad \beta = 5\gamma^2, \qquad 2\gamma + 4\delta = 5\alpha, \qquad \gamma\delta + 3\varepsilon = 5\beta,$$

ce qui donne

$$(9) \qquad \alpha = \frac{10}{3}\gamma, \qquad \beta = 5\gamma^2, \qquad \delta = \frac{11}{3}\gamma, \qquad \varepsilon = \frac{64}{9}\gamma^2.$$

On tire en outre de (8)

$$\gamma^3\varepsilon = 1728$$

relation qui, à cause de $\varepsilon = \frac{64}{9}\gamma^2$, devient

$$(10) \qquad \gamma^5 = \frac{9}{64}1728 = 3^5.$$

Pour déterminer complètement γ, il convient de faire une remarque. La valeur $-\gamma$ est celle que prend r aux centres des faces de l'icosaèdre, qui ne sont pas en même temps centres des faces de l'octaèdre déterminé par le système k_1. Or un de ces centres est certainement celui de la face 2, 9, 10 de l'icosaèdre ; il ne peut être centre d'une face de l'octaèdre, puisque précisément sur un de ses côtés (le côté 9, 10) se trouve un sommet

de l'octaèdre. Mais le centre de la face 2, 9, 10 se trouve évidemment (voir *fig.* 13 et 14, n° 75) sur l'axe réel, et, d'autre part, l'expression de r montre que r est toujours réel pour des valeurs réelles de z. Donc la valeur $-\gamma$ que prend r au centre considéré, et par suite en tous les autres centres qui ne sont pas centres des faces de l'octaèdre, est nécessairement réelle et (10) nous donne l'unique solution $\gamma = 3$.

Cela posé, on a, en vertu de (9),

$$\alpha = 10, \qquad \beta = 45, \qquad \gamma = 3, \qquad \delta = 11, \qquad \varepsilon = 64,$$

et la résolvante cherchée du cinquième degré peut s'écrire

$$Z - 1 : Z : 1 = r(r^2 + 10r + 45)^2 : (r + 3)^3(r^2 + 11r + 64) : 1728,$$

ou encore, en tenant compte des formules du n° 127,

$$\frac{T^2}{f^5} = 1728(Z - 1) = r(r^2 + 10r + 45)^2.$$

Remplaçons r par son expression (1), et écrivons pour simplifier t au lieu de t', nous aurons

$$T^2 = t^2(t^4 + 10ft^2 + 45f^2)^2,$$

puis, extrayant la racine carrée, et remarquant que pour $z_1 = 1$, $z_2 = 0$, on a

$$T = 1, \qquad t = 1,$$

il vient

$$t(t^4 + 10ft^2 + 45f^2) - T = 0, \tag{11}$$

que nous appellerons néanmoins une résolvante, bien qu'elle soit mise sous forme homogène.

149. Avant de passer à la construction d'une résolvante plus importante de l'équation de l'icosaèdre, que nous appellerons *résolvante principale*, cherchons l'expression de la forme W relative à l'octaèdre considéré précédemment, forme que nous indiquerons par W'. On a

$$W' = z_1'^8 + 14 z_1'^4 z_2'^4 + z_2'^8,$$

z_1' et z_2' étant les variables, figurant dans la substitution du paragraphe précédent. Au lieu de faire directement la substitution,

nous remarquerons que W est le hessien de t, et que le hesssien est une forme covariante. Il suffira donc de former le hessien de t', qui, à un facteur constant près, sera W'. Ecrivons W au lieu de W'; et, à cause de l'indétermination des coefficients a, b que nous introduirons un peu plus loin, on peut supprimer un facteur constant sans importance et commun à tous les termes de W. On trouve ainsi

$$W = -z_1^8 - z_1^7 z_2 - 7 z_1^6 z_2^2 + 7 z_1^5 z_2^3 - 7 z_1^3 z_2^5 - 7 z_1^2 z_2^6 + z_1 z_2^7 - z_2^8.$$

Observons que la forme

$$Y = a W + b t W,$$

où a et b sont des quantités quelconques, étant une fonction à 5 valeurs, doit satisfaire à une équation du cinquième degré

$$(1) \qquad Y^5 + AY^4 + BY^3 + CY^2 + DY + E = 0,$$

A, B, C, D, E étant des fonctions homogènes de degrés 1, 2, 3, 4, 5 en a et b, contenant z_1 et z_2. Indiquons par t_h, W_h $(h = 1, 2, 3, 4)$ les expressions de t, W relatives au système des trois médianes k_{h+1}; les t_h, W_h se déduisent de t, W au moyen de la substitution S^h, et comme l'expression de la substitution homogène S^h est

$$z'_1 = \varepsilon^{3h} z_1, \qquad z'_2 = \varepsilon^{2h} z_2,$$

on trouve

$$t_h = \varepsilon^{3h} z_1^6 - 2\varepsilon^{2h} z_1^5 z_2 - 5\varepsilon^{h} z_1^4 z_2^2 - 5\varepsilon^{4h} z_1^3 z_2^4 + 2\varepsilon^{3h} z_1 z_2^5 + \varepsilon^{2h} z_2^6,$$

$$W_h = -\varepsilon^{4h} z_1^8 - \varepsilon^{3h} z_1^7 z_2 - 7\varepsilon^{2h} z_1^6 z_2^2 + 7\varepsilon^{h} z_1^5 z_2^3$$
$$- 7\varepsilon^{4h} z_1^3 z_2^5 - 7\varepsilon^{3h} z_1^2 z_2^6 + \varepsilon^{2h} z_1 z_2^7 - \varepsilon^{h} z_2^8.$$

Si t_0 et W_0 désignent t et W, on peut dire que les racines de (1) sont

$$Y_h = a W_h + b t_h W_h \qquad (h = 0, 1, 2, 3, 4).$$

Posons donc

$$S_i = \sum_{h=0}^{4} Y_h^i \qquad (i = 1, 2, 3, 4, 5).$$

Les formules de NEWTON [1] donnent

$$\begin{aligned} A &= - \quad S_1, \\ 2B &= - \quad S_2 + S_1^2, \\ 6C &= -2S_3 + 3S_1S_2 - S_1^3, \\ 24D &= -6S_4 + 8S_3S_1 - 6S_2S_1^2 + 3S_2^2 + S_1^4. \end{aligned}$$

De plus,

$$E = -\prod_{h=0}^{4} Y_h.$$

Nous avons donc tout d'abord

$$A = -\sum_{h=0}^{4} Y_h = -\left(a\sum_{h=0}^{4} W_h + b\sum_{h=0}^{4} t_h W_h\right).$$

Les expressions $\sum_{h=0}^{4} W_h$, $\sum_{h=0}^{4} t_h W_h$ étant symétriques par rapport aux cinq octaèdres, sont des fonctions rationnelles entières de z_1, z_2, invariantes dans le groupe octaédrique, et qui, étant de degré inférieur à 60, peuvent s'exprimer rationnellement à l'aide de f, H, T. Elles sont de degrés 8 et 14. Or une fonction rationnelle entière de f, H, T ne peut être de degré 8 ou 14. Donc on a nécessairement

$$A = 0.$$

De même, en tenant compte de $S_1 = 0$, on a

$$B = -\frac{1}{2}\sum_{h=0}^{4} Y_h^2 = -\frac{1}{2}\left(a^2\sum_{h=0}^{4} W_h^2 + 2ab\sum_{h=0}^{4} t_h W_h^2 + b^2\sum_{h=0}^{4} t_h^2 W_h^2\right).$$

Les fonctions figurant dans les trois termes de la dernière expression devraient être de degrés 16, 22, 28; or, cela est impossible pour une fonction formée à l'aide des f, H, T. Donc

$$B = 0.$$

---

(1) Les *formules* de NEWTON lient les *fonctions symétriques simples* c_h (somme de plusieurs quantités, de leurs produits deux à deux, trois à trois, etc.) aux *fonctions symétriques complètes* S_h (somme des puissances semblables); elles peuvent se résumer dans la formule suivante:

$$hc_h = s_1 c_{h-1} - s_2 c_{h-2} + s_3 c_{h-3} - \ldots - (-1)^h s_h.$$

Passons au calcul de C. Comme

$$S_1 = S_2 = 0,$$

$$C = -\frac{1}{3} S_3$$
$$= -\frac{1}{3}\left(a^3 \sum_{h=0}^{4} W_h^3 + 3a^2b \sum_{h=0}^{4} t_h W_h^3 + 3ab^2 \sum_{h=0}^{4} t_h^2 W_h^3 + b^3 \sum_{h=0}^{4} t_h^3 W_h^3\right).$$

Les quatre termes sont respectivement de degrés 24, 30, 36, 42. Or, les seules fonctions qu'on puisse former avec f, H, T, et qui soient respectivement des degrés précédents, sont

$$f^2, \quad T, \quad f^3, \quad fT, .$$

d'où, en désignant par α_0, α_1, α_2, α_8 quatre constantes,

$$\sum_{h=0}^{4} W_h^3 = \alpha_0 f^2, \qquad \sum_{h=0}^{4} t_h W_h^3 = \alpha_1 T,$$
$$\sum_{h=0}^{4} t_h^2 W_h^3 = \alpha_2 f^3, \qquad \sum_{h=0}^{4} t_h^3 W_h^3 = \alpha_3 fT.$$

Pour déterminer ces constantes, il suffit d'égaler les termes de plus haut degré en z_1 dans les deux membres de chaque équation.

Dans le second membre de la première, le terme de plus haut degré en z_1 est $\alpha_0 z_1^{22} z_2^2$. D'autre part,

$$W_h^3 = -\varepsilon^{2h} z_1^{24} - 3\varepsilon^h z_1^{23} z_2 - 24 z_1^{22} z_2^2 - 22\varepsilon^{4h} z_1^{21} z_2^3 + \ldots,$$

et comme, $\sum_{h=0}^{4} \varepsilon^{rh} = 0$ pour $r \not\equiv 0 \pmod 5$, le terme de plus haut degré dans $\sum_{h=0}^{4} W_h^3$ est $-5.24\, z_1^{22} z_2^2$; il en résulte

$$\alpha_0 = -120.$$

Dans la deuxième équation le premier terme du second membre est $\alpha_1 z_1^{30}$, le premier terme du premier membre $-5z_1^{30}$, d'où $\alpha_1 = -5$.

Dans la troisième équation, le premier terme du second membre est $\alpha_2 z_1^{33} z_2^3$. Quant au premier membre, on a

$$t_h^2 W_h^3 = (\varepsilon^h z_1^{12} - 4 z_1^{11} z_2 - 6\varepsilon^{4h} z_1^{10} z_2^2 + 20\varepsilon^{3h} z_1^9 z_2^3 + \ldots)$$
$$\times (-\varepsilon^{2h} z_1^{24} - 3\varepsilon^h z_1^{23} z_2 - 24 z_1^{22} z_2^2 - 22\varepsilon^{4h} z_1^{21} z_2^3 + \ldots).$$

Le terme en $z_1^{33} z_2^3$ a pour coefficient 72, donc le même terme dans la somme $\sum_{h=0}^{4} t_h^2 W_h^3$ aura pour coefficient 360, de sorte que

$$\alpha_2 = 360.$$

Enfin, dans la dernière équation le premier terme du second membre est $\alpha_3 z_1^{41} z_2$. D'autre part,

$$t_h W_h = -\varepsilon^{2h} z_1^{14} + \varepsilon^h z_1^{13} z_2 + 26\varepsilon^{4h} z_1^{11} z_2^3 + \ldots,$$

d'où

$$t_h^3 W_h^3 = -\varepsilon^h z_1^{42} + 3 z_1^{41} z_2 + \ldots,$$

et le coefficient de $z_1^{41} z_2$ dans $\sum_{h=0}^{4} t_h^3 W_h^3$ est 15, par suite $\alpha_3 = 15$. Donc

$$C = -\frac{1}{3}(-120 a^3 f^2 - 15 a^2 b T + 1080 ab^2 f^3 + 15 b^3 f T)$$

ou bien

$$C = 5(8 a^3 f^2 + a^2 b T - 72 ab^2 f^3 - b^3 f T).$$

Faisons pour D un calcul analogue. Puisque $S_1 = S_2 = 0$, on a,

$$D = -\frac{1}{4} S_4 = -\frac{1}{4}\left(a^4 \sum_{h=0}^{4} W_h^4 + 4 a^3 b \sum_{h=0}^{4} t_h W_h^4 + 6 a^2 b \sum_{h=0}^{4} t_h^2 W_h^4 \right.$$
$$\left. + 4 ab^3 \sum_{h=0}^{4} t_h^3 W_h^4 + b^4 \sum_{h=0}^{4} t_h^4 W_h^4 \right).$$

Les cinq termes sont respectivement de degrés 32, 38, 44, 50, 56. On ne peut former avec f, H, T aucune fonction de degré 38; les seules fonctions de degrés 32, 44, 50, 56 sont les suivantes :

$$f\mathrm{H}, \quad f^2\mathrm{H}, \quad \mathrm{HT}, \quad f^3\mathrm{H}.$$

On a donc, β_0, β_2, β_3, β_4 désignant des constantes,

$$\sum_{h=0}^{4} W_h^4 = \beta_0 f \mathrm{H}, \qquad \sum_{h=0}^{4} t_h W_h^4 = 0, \qquad \sum_{h=0}^{4} t_h^2 W_h^4 = \beta_2 f^2 \mathrm{H},$$
$$\sum_{h=0}^{4} t_h^3 W_h^4 = \beta_3 \mathrm{HT}, \qquad \sum_{h=0}^{4} t_h^4 W_h^4 = \beta_4 f^3 \mathrm{H}.$$

Dans la première équation, le premier terme du second membre

est $-\beta_0 z_1^{31} z_2$. Quant au premier membre, on a

$$W_h^4 = \varepsilon^h z_1^{32} + 4 z_1^{31} z_2 + 34 \varepsilon^{4h} z_1^{30} z_2^2 + \ldots;$$

par suite, le premier terme du premier membre est $20 z_1^{31} z_2$, d'où

$$\beta_0 = -20.$$

Dans la troisième équation, le premier terme du second membre est $-\beta_2 z_1^{42} z_2^2$. D'autre part, en revenant à l'expression de t_h^2, on a

$$t_h^2 W_h^2 = (\varepsilon^h z_1^{12} - 4 z_1^{11} z_2 - 6 \varepsilon^{4h} z_1^{10} z_2^2 + \ldots) \times (\varepsilon^h z_1^{32} + 4 z_1^{31} z_2 + 34 \varepsilon^{4h} z_1^{30} z_2^2 + \ldots) = \varepsilon^{2h} z_1^{44} + 12 z_1^{42} z_2^2 + \ldots;$$

d'où

$$\beta_2 = -60.$$

Dans la quatrième équation, les premiers termes sont : pour le second membre $-\beta_3 z_1^{50}$, pour le premier membre $5 z_1^{50}$, d'où

$$\beta_3 = -5.$$

Dans la dernière équation, le premier terme du second membre est $-\beta_4 z_1^{53} z_2^3$. Quant au premier membre, écrivons pour un instant, de la façon suivante, l'expression trouvée de $t_h W_h$:

$$t_h W_h = p z_1^{14} + q z_1^{13} z_2 + r z_1^{12} z_2^2 + s z_1^{11} z_2^3 + \ldots.$$

Le coefficient de $z_1^{53} z_2^3$ dans $t_h^4 W_h^4$ est, on le voit facilement,

$$4p^3 s + 4q^3 p + 12 p^2 q r.$$

Or

$$p = -\varepsilon^{2h}, \qquad q = \varepsilon^h, \qquad r = 0, \qquad s = 26 \varepsilon^{4h}.$$

Le coefficient cherché est donc -108, et l'on a

$$\beta_4 = 540.$$

Donc

$$D = -\frac{1}{4}(-20 a^4 f H - 360 a^2 b^2 f^2 H - 20 a b^3 H T + 540 b^4 f^3 H),$$

ou bien

$$D = 5(a^4 f H + 18 a^2 b^2 f^2 H + a b^3 H T - 27 b^4 f^3 H).$$

Pour trouver l'expression de E, nous suivrons une autre voie. On a

$$E = -\prod_{h=0}^{4} Y_h = -\prod_{h=0}^{4} W_h \prod_{h=0}^{4} (a + b t_h) = b^5 \prod_{h=0}^{4} W_h \prod_{h=0}^{4} \left(-\frac{a}{b} - t_h\right).$$

Or $\prod_{h=0}^{4}$ est une forme icosaédrique de degré 40 et ne diffère par conséquent de H^2 que par un facteur constant. Si l'on observe maintenant que le premier terme de H^2 est z_1^{40} et que le premier terme de $\prod_{h=0}^{4} W_h$ est $-z_1^{40}$, on voit que ce facteur constant est -1, d'où

$$\prod_{h=0}^{4} W_h = -H^2.$$

En ce qui concerne l'autre facteur, souvenons-nous que les t^h sont les racines de l'équation (11) (n° 148, p. 276), en sorte que, u étant une indéterminée quelconque,

$$\prod_{h=0}^{4}(u-t_h) = u(u^4+10fu^2+45f^2)-T,$$

d'où

$$b^5\prod_{h=0}^{4}\left(-\frac{a}{b}-t_h\right) = -(a^5+10a^3b^2f+45ab^4f^2+b^5T)$$

et enfin

$$E = a^5H^2+10a^3b^2fH^2+45ab^4f^2H^2+b^5H^2T.$$

L'équation cherchée est donc

$$\begin{aligned} &Y^5+5(8a^3f^2+a^2bT-72ab^2f^3-b^3fT)Y^2\\ &\quad+5(a^4fH+18a^2b^2f^2H+ab^3HT-27b^4f^3H)Y\\ &\quad+a^5H^2+10a^3b^2fH^2+45ab^4f^2H^2+b^5H^2T=0. \end{aligned}$$

De là on peut obtenir une résolvante au sens ordinaire du mot, en prenant pour a, b des fonctions de z_1, z_2 telles que Y devienne de degré zéro, c'est-à-dire soit une fonction de la seule variable z. Pour cela, il suffit de poser, en désignant par m, n deux constantes,

$$a = \frac{12mf}{H}, \qquad b = \frac{144nf^3}{TH} \quad (^1).$$

---

(1) Il est essentiel pour cela que a soit de degré -8 et b de degré -14. Or, les fonctions invariantes les plus simples de ce degré sont précisément $\frac{f}{H}$ et $\frac{f^3}{TH}$.

Introduisons les deux fonctions de z

$$u = \frac{12 f^2 t}{T}, \qquad v = \frac{12 f W}{H},$$

invariantes dans le sous-groupe tétraédrique considéré, et tenant compte (n° 127) de la relation

$$Z - 1 : Z : 1 = T^2 : -H^3 : 12^3 f^5,$$

on a

$$Y = mv + nuv,$$

et l'équation devient

$$\begin{aligned} Y^5 &- \frac{5}{Z}\left(8m^3 + 12m^2 n + \frac{6mn^2 + n^3}{1 - Z}\right) Y^2 \\ &+ \frac{15}{Z}\left[-4m^3 + \frac{6m^2n^2 + 4mn^3}{1 - Z} + \frac{3}{2}\,\frac{n^4}{(1 - Z)^2}\right] Y \\ &- \frac{3}{Z}\left[48m^5 - \frac{40m^3n^2}{1 - Z} + \frac{15mn^4 + 4n^5}{(1 - Z)^2}\right] = 0. \end{aligned}$$

C'est une équation de la forme

$$Y^5 + 5\alpha Y^2 + 5\beta Y + \gamma = 0,$$

dont le discriminant a pour expression

$$5^2(108\alpha^5\gamma - 135\alpha^4\beta^2 + 90\alpha^2\beta\gamma^2 - 320\alpha\beta^3\gamma + 256\beta^5 + \gamma^4) \quad (^1).$$

---

(1) Voici un procédé assez simple pour obtenir le discriminant. Cherchons à former le résultant de l'équation

$$\varphi \equiv Y^5 + 5\alpha Y^2 + 5\beta Y + \gamma = 0$$

et de sa dérivée. Au lieu de ces deux équations, on peut prendre

$$\frac{1}{5}\varphi' \equiv Y^4 + 2\alpha Y + \beta = 0, \qquad \psi \equiv -\frac{1}{5}\varphi' Y + \varphi \equiv 3\alpha Y^2 + 4\beta Y + \gamma = 0,$$

ou encore les deux suivantes :

$$\psi = 0, \qquad \chi \equiv \frac{2}{5}\beta\varphi' - \alpha\psi \equiv 2\beta Y^4 - 3\alpha^2 Y^2 + 2\beta^2 - \alpha\gamma = 0.$$

De la première on tire

$$-4\beta Y = 3\alpha Y^2 + \gamma,$$

puis

$$16\beta^2 Y^2 = 9\alpha^2 Y^5 + 6\alpha\gamma Y^2 + \gamma^2$$

ou bien

$$\omega \equiv 9\alpha^2 Y^4 + (6\alpha\gamma - 16\beta^2) Y^2 + \gamma^2 = 0.$$

On sait que le résultant de $\omega = 0$, $X = 0$ est (*voir* par exemple Pascal, *Reper-*

Observons que la racine carrée du discriminant, étant le produit des différences des racines, est une fonction symétrique des W_h, t_h, et par conséquent une fonction rationnelle de f, H, T. Il serait un peu long de former l'expression analytique de cette fonction qui ne présente aucun intérêt pour nous.

150. Cherchons maintenant une résolvante du sixième degré de l'équation icosaédrique.

Le groupe icosaédrique comprend six sous-groupes diédriques équivalents d'ordre 10. L'un d'eux a pour substitutions génératrices S, U, et les autres s'en déduisent en appliquant les substitutions

$$T,\quad TS,\quad TS^2,\quad TS^3,\quad TS^4$$

qui transforment la diagonale 1.2 en les autres diagonales

$$2.7\quad 3.8\quad 4.9\quad 5.10\quad 6.11.$$

---

torio di matematiche superiori, vol. I, p. 108)

$$\begin{vmatrix} -27\alpha^4 - 2\beta(6\alpha\gamma - 16\beta^2) & 9\alpha^2(2\beta^2 - \alpha\gamma) - 2\beta\gamma^2 \\ 9\alpha^2(2\beta^2 - \alpha\gamma) - 2\beta\gamma^2 & (2\beta^2 - \alpha\gamma)(6\alpha\gamma - 16\beta^2) + 3\alpha^2\gamma^2 \end{vmatrix}$$
$$= \begin{vmatrix} -27\alpha^4 + 32\beta^3 - 12\alpha\beta\gamma & 18\alpha^2\beta^2 - 9\alpha^3\gamma - 2\beta\gamma^2 \\ 18\alpha^2\beta^2 - 9\alpha^3\gamma - 2\beta\gamma^2 & 28\alpha\beta^2\gamma - 32\beta^4 - 4\alpha^2\gamma^2 \end{vmatrix} = 0$$

ou, supprimant le facteur $-4\beta^2$,

$$108\alpha^5\gamma - 135\alpha^4\beta^2 + 90\alpha^2\beta\gamma^2 - 320\alpha\beta^3\gamma + 256\beta^5 + \gamma^4 = 0.$$

Représentons ensuite par $\Delta^2(Y)$ le discriminant, c'est-à-dire le produit des carrés des différences des racines, et par k un facteur numérique, que nous déterminerons dans un instant, on a

$$\Delta^2(Y) = k[108\alpha^5\gamma - 135\alpha^4\beta^2 + 90\alpha^2\beta\gamma^2 - 320\alpha\beta^3\gamma + 256\beta^5 + \gamma^4].$$

Pour calculer k, prenons un cas particulier. Supposons $\alpha = \gamma = 0$, $5\beta = -1$, en sorte que les racines de l'équation sont ± 1, $\pm i$, 0.

Comme $\Delta(Y)$ est le déterminant de VANDERMONDE, on a

$$\Delta(Y) = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & 0 \\ 1 & 1 & -1 & -1 & 0 \\ 1 & -1 & -i & i & 0 \\ 1 & 1 & 1 & 1 & 0 \end{vmatrix} = -16i,$$

tandis que $\Delta^2(Y) = -\frac{256}{5^5}k$, d'où il résulte $k = 5^5$.

Les substitutions S, U, mises sous forme homogène, s'écrivent

$$z'_1 = \varepsilon^3 z_1, \qquad z'_2 = \varepsilon^2 z_2; \qquad z'_1 = -z_2, \qquad z'_2 = z_1$$

et toutes deux nous donnent

$$(z'_1 z'_2)^2 = (z_1 z_2)^2,$$

de sorte que $\varphi = 5 z_1^2 z_2^2$ est une fonction invariante pour les substitutions du sous-groupe diédrique considéré. Soit

$$(1) \qquad \varphi^6 + A\varphi^5 + B\varphi^4 + \varphi^3 + D\varphi^2 + E\varphi + F = 0$$

la résolvante; A, B, C, D, E, F seront des formes invariantes respectivement dans les groupes icosaédriques de degrés 4, 8, 12, 16, 20, 24. Comme ces formes doivent s'exprimer à l'aide de f, H, T, on aura

$$A = B = D = 0,$$
$$C = \alpha f, \qquad E = \beta H, \qquad F = \gamma f^2,$$

α, β, γ étant trois constantes. L'équation (1) devient donc

$$\varphi^6 + \alpha f \varphi^3 + \beta H \varphi + \gamma f^2 = 0.$$

Pour déterminer α, β, γ, remplaçons φ, f, A par leurs expressions; nous aurons

$$\begin{aligned} 5^6 z_1^{12} z_2^{12} &+ \alpha.5^3 z_1^6 z_2^6 (z_1^{11} z_2 - 11 z_1^6 z_2^6 - z_1 z_2^{11}) \\ &+ \beta.5 z_1^2 z_2^2 (-z_1^{20} - 228 z_1^{15} z_2^5 - 494 z_1^{10} z_2^{10} + \ldots) \\ &+ \gamma(z_1^{22} z_2^2 - 22 z_1^{17} z_2^7 + 119 z_1^{12} z_2^{12} - \ldots) = 0. \end{aligned}$$

En annulant les coefficients de $z_1^{22} z_2^2$, $z_1^{17} z_2^7$, $z_1^{12} z_2^{12}$, on obtient les relations

$$-5\beta + \gamma = 0, \qquad 5^3\alpha - 5.228\beta - 22\gamma = 0,$$
$$5^6 - 5^3.11\alpha - 5.494\beta + 119\gamma = 0$$

qui, résolues, donnent

$$\alpha = 10, \qquad \beta = 1, \qquad \gamma = 5.$$

L'équation cherchée est donc

$$(2) \qquad \varphi^6 + 10 f \varphi^3 + H\varphi + 5 f^2 = 0.$$

Pour avoir une vraie résolvante, on pose

$$\varphi = \frac{12 f^2 \zeta}{H},$$

où ζ est fonction de la seule variable z, d'où

$$\zeta^6 - 10Z\zeta^3 + 12Z^2\zeta + 5Z^2 = 0.$$

On peut donner à la résolvante uue autre forme, en posant dans (2)

$$\varphi^3 = -f\xi \tag{3}$$

et écrivant (2) de la façon suivante

$$-H\varphi = \varphi^6 + 10f\varphi^3 + 5f^2,$$

d'où

$$(\varphi^6 + 10f\varphi^3 + 5f^2)^3 + H^3\varphi^3 = 0. \tag{4}$$

Moyennant la substitution (3) l'équation (4) devient

$$(\xi^2 - 10\xi + 5)^3 + 1728Z\xi = 0,$$

ou bien

$$Z = \frac{(\xi^2 - 10\xi + 5)^3}{-1828\xi}$$

ou encore

$$Z - 1 = \frac{(\xi^2 - 10\xi + 5)^3 + 1728\xi}{-1728\xi}. \tag{5}$$

Pour décomposer le numérateur en un produit de facteurs, utilisons une remarque géométrique.

Les substitutions du sous-groupe considéré échangent entre elles les milieux des arêtes suivantes :

(*a*)	1.2,	1.3,	1.4,	1.5,	1.6,	7.12,	8.12,	9.12,	10.12,	11.12;
(*b*)	2.3,	3.4,	4.5,	5.6,	6.2,	7.8,	8.9,	9.10,	10.11,	11.7;
(*c*)	2.10,	3.11,	4.7,	5.8,	6.9;					
(*d*)	2.9,	3.10,	4.11,	5.7,	6.8.					

Le numérateur de (5), devant s'annuler aux milieux des arêtes, puisqu'en ces points $Z = 1$, les six racines se composent de deux racines doubles et deux racines simples. On posera donc

$$(\xi^2 - 10\xi + 5)^3 + 1728\xi = (\xi^2 + \alpha\xi + \beta)^2(\xi^2 + \gamma\xi + \delta),$$

ce qui donne

$$(6)\quad \left\{\begin{aligned} -30 &= 2\alpha + \gamma, \\ 315 &= \alpha^2 + 2\alpha\gamma + 2\beta + \delta, \\ -1300 &= \alpha^2\gamma + 2\alpha\beta + 2\beta\gamma + 2\alpha\delta, \\ 1575 &= \alpha^2\delta + 2\alpha\beta\gamma + 2\beta\delta + \beta^2, \\ 978 &= \beta^2\gamma + 2\alpha\beta\delta, \\ 125 &= \beta^2\delta. \end{aligned}\right.$$

Au lieu de procéder à la résolution directe des équations (6), admettons *a priori* qu'elles aient une solution formée de nombres entiers. Alors la dernière ne peut admettre que les solutions

$$\beta = \pm 5, \quad \delta = 5; \qquad \beta = \pm 1, \quad \delta = 125.$$

D'autre part la première donne $\alpha \equiv \gamma \pmod 3$ et par suite la seconde $\beta \equiv \delta \pmod 3$, de sorte que parmi ces quatre solutions, il n'y a que deux solutions possibles :

$$\beta = 5, \quad \delta = 5; \qquad \beta = -1, \quad \delta = 125.$$

Pour $\beta = 5$, $\delta = 5$ le second membre de l'avant-dernière équation (6) serait multiple de 5, tandis que le premier membre ne l'est pas. Cette dernière solution est à rejeter et si l'on a

$$\beta = -1, \quad \delta = 125.$$

Les équations (6) donnent ensuite

$$\alpha = -4, \quad \gamma = -22,$$

et la résultante cherchée est

$$Z-1 : Z : 1 = (\xi^2 - 4\xi - 1)^2(\xi^2 - 22\xi + 125) : (\xi^2 - 10\xi + 5)^3 : (-1728\xi).$$

151. La notion de résolvante s'étend à l'équation modulaire.

Soit Γ_s un sous-groupe d'indice fini s du groupe modulaire, toute fonction invariante u dans ce sous-groupe est liée à J par une équation algébrique

$$f(u, \mathrm{J}) = 0 \tag{1}$$

de degré s par rapport à u. On peut appeler cette équation une *résolvante* de l'équation modulaire, en ce sens que, une fois cette équation (1) résolue, c'est-à-dire une fois trouvée l'expression de la fonction u de J, il suffira de savoir exprimer z au moyen de u pour avoir en même temps l'expression de z à l'aide de J. En d'autres termes, une fois l'équation (1) résolue, la résolution de l'équation modulaire principale

$$\mathrm{J} = \mathrm{J}(z)$$

est ramenée à la résolution de l'équation modulaire relative au sous-groupe Γ_s

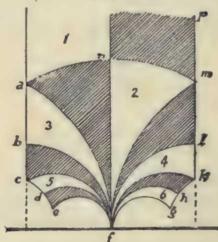
$$u = u(z),$$

et ce problème peut être regardé comme plus simple que le précédent, puisque le réseau de Γ_s est plus simple que celui de Γ.

L'équation diédrique pour $m = 3$, et les équations tétraédrique, octaédrique et icosaédrique sont les résolvantes de l'équation modulaire correspondant aux sous-groupes $\Gamma_{[2]}$, $\Gamma_{[3]}$, $\Gamma_{[4]}$, $\Gamma_{[5]}$.

Nous formerons, comme exemples de résolvantes, deux autres résolvantes, l'une du cinquième, l'autre du sixième degré, correspondant au sous-groupe $\Gamma_{[5]}$. Elles sont nécessairement équivalentes à l'équation icosaédrique; nous trouverons en effet qu'elles coïncident avec deux des résolvantes équivalentes déjà construites.

Fig. 47.



Nous avons vu (n° 113) que, p étant un nombre premier, $G_{\mu(p)}$ contient $p+1$ sous-groupes hémimétacycliques $G_{\frac{p(p-1)}{2}}$; auxquels correspondent autant de sous-groupes de Γ d'indice $p+1$. En particulier pour $p = 5$, on a 6 sous-groupes d'indice 6, contenant tous le sous-groupe $\Gamma_{[5]}$. L'un d'eux est formé des substitutions modulaires permutables avec le groupe cyclique engendré par S et par suite contient S elle-même. Il suit de là que son champ fondamental est compris tout entier dans une bande de largeur 1 parallèle à l'axe imaginaire. L'expression générale des substitutions du sous-groupe est (n° 109)

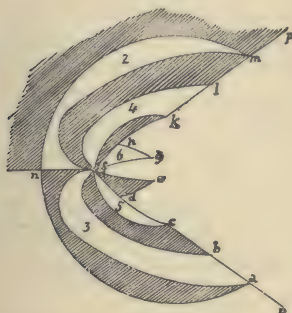
$$z' \equiv \frac{\alpha z + \beta}{\alpha^{-1}} \qquad (\text{mod}\, 5);$$

Il est facile de voir que le groupe est permutable avec la pseudo-substitution $z' = -\bar{z}$, de sorte que l'on peut prendre pour champ fondamental un champ symétrique par rapport à l'axe imaginaire.

Or ce champ est connexe et comprend douze bitriangles en prenant le bitriangle 1 comme bitriangle initial, on obtient immédiatement le champ représenté par la figure 47.

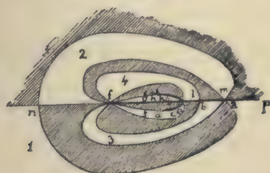
Par une déformation continue, dont la figure 48 nous offre une

Fig. 48.



phase intermédiaire, on peut amener le champ à recouvrir entièrement un plan, que nous appellerons le plan u. On fera en sorte que l'axe imaginaire du plan z, conservant sa forme rectiligne, vienne à coïncider avec l'axe réel du plan u, et que tous les nœuds du champ viennent tomber sur cet axe, à l'exception des nœuds d

Fig. 49.



et h (*fig.* 49). Alors si l'on pose $u = \frac{1}{v}$, l'équation modulaire

$$J(z) = J$$

aura une résolvante du sixième degré en v dont les coefficients seront des fonctions rationnelles de premier degré de J; en effet, à

chaque valeur de v correspond une valeur unique de J. Nous pourrons donc écrire la résolvante considérée de la façon suivante :

$$J-1 : J : 1 = \varphi(v) : \psi(v) : \chi(v),$$

$\varphi(v)$, $\psi(v)$, $\chi(v)$ étant des polynomes du sixième degré au plus.

Supposons que l'origine du plan u soit en f.

Les nœuds de première espèce sont n, d, h, bl (¹), ceux de deuxième espèce am, $cegk$; ceux de troisième espèce f, p. Les points n, b, où se croisent 4 triangles, doivent être considérés comme doubles; les points d, h, où se croisent deux triangles, sont simples. De même a, c sont triples et f est quintuple. Donc le polynome $\varphi(v)$ a deux racines doubles et deux simples, $\psi(v)$ deux racines triples, $\chi(v)$ une racine quintuple et une simple. De plus, la racine quintuple de $\chi(v)$ est $v = \infty$, la racine simple $v = 0$, en sorte que, à un facteur constant près, on a $\chi(v) = v$. Nous poserons

$$\begin{aligned}
\chi(v) &= -1728v,\\
\varphi(v) &= \lambda(v^2+\alpha v+\beta)^2(v^2+\gamma v+\delta),\\
\psi(v) &= \mu(v^2+\varepsilon v+\xi)^3.
\end{aligned}$$

La relation

$$(1) \qquad \varphi(v) = \psi(v) - \chi(v) = \psi(v) + 1728v,$$

d'où l'on tire $\lambda = \mu$, donne

$$\frac{\varphi(v)}{v} = \frac{\psi(v)}{v} + 1728,$$

et par dérivation

$$v\varphi'(v) - \varphi(v) = v\psi'(v) - \psi(v),$$

ou bien

$$\begin{aligned}
&(v^2+\alpha v+\beta)[5v^4+(3\alpha+4\gamma)v^3+(\beta+3\delta+2\alpha\gamma)v^2+\alpha\delta v-\beta\delta]\\
&\quad = (v^2+\varepsilon v+\zeta)^2(5v^2+2\varepsilon v-\zeta).
\end{aligned}$$

Puisque les trinomes $v^2+\alpha v+\beta$, $v^2+\varepsilon v+\zeta$ n'ont pas de racine commune, on doit avoir

$$5v^2+2\varepsilon v-\zeta = 5(v^2+\alpha v+\beta),$$

$$5v^4+(3\alpha+4\gamma)v^3+(\beta+3\delta+2\alpha\gamma)v^2+\alpha\delta v-\beta\delta = 5(v^2+\varepsilon v+\zeta)^2;$$

(¹) Par bl nous entendons le point où les points b et l coïncident après la déformation.

d'où

$$2\varepsilon = 5\alpha, \qquad -\zeta = 5\beta, \qquad 3\alpha + 4\gamma = 10\varepsilon,$$
$$\beta + 3\delta + 2\alpha\gamma = 5\varepsilon^2 + 10\zeta, \qquad \alpha\delta = 10\varepsilon\zeta, \qquad -\beta\delta = 5\zeta^2.$$

On trouve ainsi

$$(2) \quad \alpha = \frac{2}{5}\varepsilon, \qquad \beta = -\frac{1}{100}\varepsilon^2, \qquad \gamma = \frac{11}{5}\varepsilon, \qquad \delta = \frac{5}{4}\varepsilon^2, \qquad \zeta = \frac{1}{20}\varepsilon^2.$$

En égalant dans (1) les coefficients de v, et se rappelant que $\lambda = \mu$, il vient

$$\lambda(2\alpha\beta\delta + \beta^2\gamma - 3\varepsilon\zeta^2) - 1728 = 0,$$

et en tenant compte de (2)

$$\lambda\varepsilon^5 = -10^5.$$

Comme dans la déformation précédente il y a une certaine part d'arbitraire, le coefficient λ peut être pris à volonté. Faisons $\lambda = 1$, on a alors

$$\varepsilon^5 = -10^5.$$

Or ε est la somme changée de signe des valeurs de v, correspondant aux points a, c, valeurs qui sont réelles; donc $\varepsilon = -10$.

Les relations (2) donnent ensuite

$$\alpha = -4, \qquad \beta = -1, \qquad \gamma = -22, \qquad \delta = 125, \qquad \varepsilon = -10, \qquad \zeta = 5,$$

en sorte que la résolvante cherchée est

$$J - 1 : J : 1 = (v^2 - 4v - 1)^2(v^2 - 22v + 125) : (v^2 - 10v + 5)^3 : (-1728v).$$

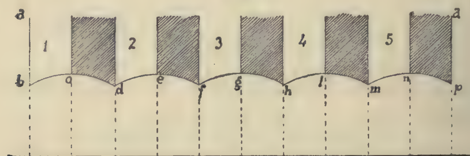
Elle est identique à la résolvante de l'équation icosaédrique formée au n° 150.

152. On peut obtenir une autre résolvante de l'équation modulaire en observant que, d'après la congruence $5 \equiv -3 \pmod 8$, $G_{\mu(5)}$ contient $\frac{5(5^2-1)}{24} = 5$ sous-groupes tétraédriques équivalents G_{12}, auxquels correspondent 5 sous-groupes équivalents Γ_5 d'indice 5 de Γ contenant tous $\Gamma_{[5]} = \Gamma_{60}$. Cette résolvante sera donc du cinquième ordre.

Comme S et ses puissances, considérées comme substitutions de $G_{\mu(5)}$ sont d'ordre 5, elles ne peuvent faire partie d'un groupe

tétraédrique; donc les bitriangles 1, S, S^2, S^3, S^4 ne peuvent être homologues entre eux dans aucun des Γ_5. On en conclut que l'ensemble de ces bitriangles (*fig.* 50) constitue un champ fonda-

Fig. 50.



mental pour un des Γ_5. En effet établissons entre les côtés de cette figure la correspondance suivante :

$$ab,\quad ap;\quad bd,\quad fd;\quad fg,\quad hg;\quad hm,\quad pm$$

Fig. 51.

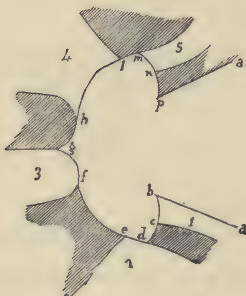
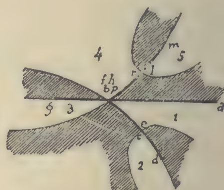


Fig. 52.



et déformons le polygone de façon à le ramener à une surface fermée, un plan par exemple; le réseau qui recouvre ce plan a pour symbole (2, 3, 5) et satisfait aux conditions du théorème d'existence des sous-groupes (n° 97), comme nous le verrons beaucoup mieux un peu plus loin en examinant chacun des nœuds. Donc il existe un sous-groupe d'indice 5, qui a pour champ fondamental le polygone donné; ce sous-groupe doit contenir $\Gamma_{[5]}$, et doit par suite coïncider avec un des 5 sous-groupes considérés. Les nœuds de première espèce sont *ce*, *g*, *ln*; ceux de deuxième espèce *bfhp*, *d*, *m*; ceux de troisième espèce se réduisent au nœud unique *a*. Les

points c, l sont doubles, g est simple; b est triple, les d et m sont simples et le point a est quintuple.

La résolvante aura donc la forme

$$J - 1 : J : 1 = \varphi(u) : \psi(u) : \chi(u)$$

avec

$$\varphi(u) = \lambda(u^2 + \alpha u + \beta)^2(u - \gamma),$$
$$\psi(u) = \mu(u^2 + \delta u + \varepsilon)(u - \zeta)^3, \qquad \chi(u) = \nu(u - \eta)^5.$$

Supposons que u représente l'affixe des points du plan sur lequel nous avons placé le réseau, que la droite afg soit l'axe réel du même plan, g étant l'origine et f ayant pour abscisse -3. Alors on aura $\eta = \infty$, $\chi(u)$ se réduira à une constante et nous pourrons poser

$$\chi(u) = 1728.$$

Puisque

$$(1) \qquad \psi(u) = \psi(u) - \chi(u),$$

nous aurons $\lambda = \mu$. De plus $\gamma = 0$, $\zeta = -3$; (1) deviendra

$$(2) \qquad \lambda u(u^2 + \alpha u + \beta)^2 = \lambda(u + 3)^3(u^2 + \delta u + \varepsilon) - 1728$$

et, en dérivant,

$$(u^2 + \alpha u + \beta)[u^2 + \alpha u + \beta + 2u(2u + \alpha)]$$
$$= (u + 3)^2[3(u^2 + \delta u + \varepsilon) + (u + 3)(2u + \delta)],$$

ou bien

$$(u^2 + \alpha u + \beta)(5u^2 + 3\alpha u + \beta)$$
$$= (u + 3)^2[5u^2 + (4\delta + 6)u + 3\varepsilon + 3\delta].$$

En raisonnant comme précédemment, on trouve

$$5(u^2 + \alpha u + \beta) = 5u^2 + (4\delta + 6)u + 3\varepsilon + 3\delta,$$
$$5u^2 + 3\alpha u + \beta = 5(u + 3)^2,$$

ce qui donne

$$5\alpha = 4\delta + 6, \qquad 5\beta = 3\varepsilon + 3\delta, \qquad 3\alpha = 30, \qquad \beta = 45,$$

d'où

$$\alpha = 10, \qquad \beta = 45, \qquad \delta = 11, \qquad \varepsilon = 64.$$

Si ensuite dans (2) nous faisons $u = 0$, il vient

$$\lambda = \frac{1728}{27\varepsilon} = 1.$$

La résolvante est donc

$$J - 1 : J : 1 = u(u^2 + 10u + 45)^2 : (u+3)^3(u^2 + 11u + 64) : 1728;$$

elle coïncide avec la résolvante de l'équation icosaédrique (n° 148).

Rapports entre les équations polyédriques et la théorie de la résolution algébrique des équations.

153. Soit une équation générale du troisième degré, que moyennant une substitution linéaire on peut supposer ramenée à la forme

$$x^3 + 3ax + 2b = 0, \tag{1}$$

ses racines x_1, x_2, x_3 satisfont à la relation

$$\sum_{i=1}^{3} x_i = 0.$$

Si l'on considère a, b comme variables; x_1, x_2, x_3 peuvent représenter les coordonnées homogènes des points de la droite (2), et à chaque permutation des x correspond une transformation projective de la droite en elle-même, c'est-à-dire une transformation linéaire de l'abscisse z des points de la droite. Les 6 permutations de x_1, x_2, x_3 donnent lieu ainsi à 6 substitutions linéaires des z, formant un groupe holoédriquement isomorphe au groupe des 6 permutations. Or un groupe de substitutions linéaires et du sixième ordre ne peut être qu'un groupe cyclique ou diédrique; mais, le groupe des 6 permutations ne pouvant être cyclique, la première hypothèse est à rejeter et par suite le groupe des 6 substitutions linéaires des z est un groupe diédrique ($m = 3$). Donc la détermination de z en fonction de a et b dépend de la résolution d'une équation diédrique du sixième degré. Une fois z fixé, les coordonnées x_1, x_2, x_3 sont déterminées d'une manière unique, et l'on peut dire *a priori* que x_1, x_2, x_3 s'exprimeront rationnellement en z.

Nous arrivons donc à la conclusion suivante :

La résolution d'une équation générale du troisième degré peut se ramener à celle d'une équation diédrique du sixième degré.

Indiquons, comme toujours, les substitutions du groupe diédrique du sixième ordre par

$$1, \quad S, \quad S^2, \quad T, \quad ST, \quad S^2T,$$

S et T désignant respectivement les substitutions

$$(3) \qquad z' = \alpha z, \qquad z' = \frac{1}{z} \qquad \left(\alpha = e^{\frac{2i\pi}{3}}\right),$$

à la substitution S nous pouvons faire correspondre dans le groupe des permutations de x_1, x_2, x_3 la permutation d'ordre trois x_2, x_3, x_1, et à T la permutation x_1, x_3, x_2 d'ordre deux. Comme z est une fonction linéaire de x_1, x_2, x_3, nous poserons

$$(4) \qquad z = \frac{a_1 x_1 + a_2 x_2 + a_3 x_3}{b_1 x_1 + b_2 x_2 + b_3 x_3}.$$

Appliquant à z les substitutions (3) et aux x les permutations correspondantes, on a

$$(5) \qquad \left\{ \begin{aligned} \alpha z &= \frac{a_1 x_2 + a_2 x_3 + a_3 x_1}{b_1 x_2 + b_2 x_3 + b_3 x_1}, \\ \frac{1}{z} &= \frac{a_1 x_1 + a_2 x_3 + a_3 x_2}{b_1 x_1 + b_2 x_3 + b_3 x_2}, \end{aligned} \right.$$

et en comparant (4) et (5) on obtient

$$(6) \qquad \frac{\alpha a_1}{a_3} = \frac{\alpha a_2}{a_1} = \frac{\alpha a_3}{a_2} = \frac{b_1}{b_3} = \frac{b_2}{b_1} = \frac{b_3}{b_2},$$

$$(7) \qquad \frac{a_1}{b_1} = \frac{a_2}{b_3} = \frac{a_3}{b_2} = \frac{b_1}{a_1} = \frac{b_2}{a_3} = \frac{b_3}{a_2}.$$

Soit β la valeur commune des rapports (6), ε celle des rapports (7); on trouve immédiatement

$$\beta = \sqrt[3]{1}, \qquad \varepsilon = \sqrt{1},$$

de plus

$$a_2 = \alpha^2 \beta a_1, \qquad a_3 = \alpha \beta^2 a_1, \qquad b_2 = \beta b_1,$$
$$b_3 = \beta^2 b_1, \qquad b_1 = \varepsilon a_1, \qquad \beta = \alpha^2,$$

on peut donc poser

$$a_1 = 1, \quad a_2 = \alpha, \quad a_3 = \alpha^2, \quad b_1 = \varepsilon, \quad b_2 = \varepsilon\alpha^2, \quad b_3 = \varepsilon\alpha.$$

Il est facile de s'assurer qu'il est indifférent de prendre pour ε l'une ou l'autre des valeurs ± 1; prenons par exemple $\varepsilon = +1$, alors

$$z = \frac{x_1 + \alpha x_2 + \alpha^2 x_3}{x_1 + \alpha^2 x_2 + \alpha x_3}.$$

Posons

$$(8) \qquad x_1 + \alpha x_2 + \alpha^2 x_3 = p, \qquad x_1 + \alpha^2 x_2 + \alpha x_3 = q,$$

d'où

$$z = \frac{p}{q}.$$

Les relations (2) et (8) donnent, en vertu des propriétés connues des racines de l'unité,

$$(9) \quad x_1 = \frac{1}{3}(p + q), \qquad x_2 = \frac{1}{3}(\alpha^2 p + \alpha q), \qquad x_3 = \frac{1}{3}(\alpha p + \alpha^2 q);$$

de plus

$$\begin{aligned} pq &= x_1^2 + x_2^2 + x_3^2 - x_2 x_3 - x_3 x_1 - x_1 x_2 \\ &= (x_1 + x_2 + x_3)^2 - 3(x_2 x_3 + x_3 x_1 + x_1 x_2) \\ &= -3(x_2 x_3 + x_3 x_1 + x_1 x_2) \\ &= -9a; \end{aligned}$$

$$\begin{aligned} p^3 + q^3 &= 2(x_1^3 + x_2^3 + x_3^3) + 12 x_1 x_2 x_3 \\ &\quad - 3(x_2^2 x_3 + x_3^2 x_2 + x_3^2 x_1 + x_1^2 x_3 + x_1^2 x_2 + x_2^2 x_1) \\ &= 2(x_1 + x_2 + x_3)^3 \\ &\quad - 9[x_2 x_3 (x_2 + x_3) + x_3 x_1 (x_3 + x_1) + x_1 x_2 (x_1 + x_2)] \\ &= 27 x_1 x_2 x_3 \\ &= -54 b, \end{aligned}$$

ou bien

$$(10) \qquad a = -\frac{pq}{9}, \qquad b = -\frac{p^3 + q^3}{54}.$$

Introduisant ces valeurs dans l'équation diédrique à laquelle satisfait z

$$Z = \frac{(z^3 + 1)^2}{4 z^3} = \frac{(p^3 + q^3)^2}{4 p^3 q^3},$$

on obtient pour Z la valeur

$$Z = -\frac{b^2}{a^3}.$$

D'autre part les relations (10) peuvent s'écrire

$$a = -\frac{1}{9} z q^2, \qquad b = -\frac{1}{54}(z^3+1)q^3,$$

d'où

$$\frac{b}{a} = \frac{1}{6}\,\frac{z^3+1}{z}\,q,$$

et par suite

$$q = \frac{6b}{a}\,\frac{z}{z^3+1}, \qquad p = \frac{6b}{a}\,\frac{z^2}{z^3+1},$$

et en remplaçant dans (9) p et q par les valeurs précédentes, on obtient les expressions suivantes de x_1, x_2, x_3 en fonction rationnelle de z :

$$(11) \quad x_1 = \frac{2b}{a}\,\frac{z(z+1)}{z^3+1}, \qquad x_2 = \frac{2b}{a}\,\frac{\alpha z(\alpha z+1)}{z^3+1}, \qquad x_3 = \frac{2b}{a}\,\frac{\alpha^2 z(\alpha^2 z+1)}{z^3+1}.$$

Si l'on résout l'équation diédrique, on a (n° **147**)

$$z = \sqrt[3]{2Z - 1 + 2\sqrt{Z(Z-1)}} = \frac{1}{a}\sqrt[3]{-2b^2 - a^3 + 2b\sqrt{b^2+a^3}}$$
$$= -\frac{1}{a}\left(b - \sqrt{b^2+a^3}\right)^{\frac{2}{3}},$$

et, en remplaçant z par cette valeur dans les formules (11), on obtient les formules de résolution de l'équation (1).

154. Avant d'exposer la résolution de l'équation générale du quatrième degré, observons que le groupe des 24 permutations de 4 éléments est holoédriquement isomorphe au groupe octaédrique. En effet, il contient l'opération (2341) d'ordre 4 et l'opération (1243) d'ordre 2, dont le produit est l'opération (2431) d'ordre 3 (n° **104**).

Pour réaliser cet isomorphisme, affectons les 4 sommets d'un tétraèdre régulier des indices 1, 2, 3, 4 et faisons correspondre à chaque rotation du tétraèdre sur lui-même la permutation des sommets qui en résulte. Il est facile de s'assurer que les 12 permutations correspondantes sont toutes paires. Faisons ensuite correspondre à une quelconque des rotations, qui changent le tétraèdre en son tétraèdre polaire, une quelconque des permu-

tations impaires des quatre indices 1, 2, 3, 4, nous aurons complété ainsi l'isomorphisme.

Les trois rotations d'ordre 2 du groupe tétraédrique ayant pour axes les trois médianes, chacune d'elles échange les sommets deux à deux. Il leur correspond donc les permutations (2143), (3412), (4321).

Nous supposerons les indices dont sont affectés les sommets, placés dans un ordre tel qu'à la rotation U corresponde la permutation (2143), et nous ferons correspondre à la rotation V la permutation impaire (2341).

Cela posé, prenons l'équation du quatrième degré sous la forme dite *principale*

$$x^4 + 4ax + b = 0, \tag{1}$$

à laquelle se ramène l'équation générale, moyennant la résolution d'une équation du second degré, ainsi que nous le verrons plus loin. Les 4 racines x_1, x_2, x_3, x_4 satisfont alors aux relations

$$\sum_{i=1}^{4} x_i = 0, \qquad \sum_{i=1}^{4} x_i^2 = 0, \tag{2}$$

et, en considérant les x comme les coordonnées homogènes d'un point de l'espace, on voit que les 24 points correspondant à chacune des équations (1) sont situés sur la conique (2), que nous appellerons *conique principale*.

Proposons-nous de construire une fonction linéaire z des x_i, qui, par les permutations des x_i, subisse les substitutions correspondantes du groupe octaédrique.

Il suffira naturellement de s'assurer que cela a lieu pour les deux permutations (2341), (2143) qu'on a fait correspondre aux substitutions V et U du groupe octaédrique. Rappelons que les expressions de ces deux substitutions sont (n° 64)

$$z' = iz, \qquad z = \frac{1}{z}.$$

Posons

$$z = \frac{a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4}{b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4}.$$

On devra avoir

$$(3)\qquad \frac{a_1x_2+a_2x_3+a_3x_4+a_4x_1}{b_1x_2+b_2x_3+b_3x_4+b_4x_1} = i\,\frac{a_1x_1+a_2x_2+a_3x_3+a_4x_4}{b_1x_1+b_2x_2+b_3x_3+b_4x_4},$$

$$(4)\qquad \frac{a_1x_2+a_2x_1+a_3x_4+a_4x_3}{b_1x_2+b_2x_1+b_3x_4+b_4x_3} = \frac{b_1x_1+b_2x_2+b_3x_3+b_4x_4}{a_1x_1+a_2x_2+a_3x_3+a_4x_4}.$$

Pour que la relation (3) soit satisfaite identiquement, il suffit de poser

$$\frac{a_4}{ia_1} = \frac{a_1}{ia_2} = \frac{a_2}{ia_3} = \frac{a_3}{ia_4} = \frac{b_4}{b_1} = \frac{b_1}{b_2} = \frac{b_2}{b_3} = \frac{b_3}{b_4}.$$

Soit γ la valeur commune de ces rapports, on trouve

$$\gamma^4 = 1,$$

$$a_2 = -i\gamma^3 a_1, \qquad a_3 = -\gamma^2 a_1, \qquad a_4 = i\gamma a_1,$$

$$b_2 = \gamma^3 b_1, \qquad b_3 = \gamma^2 b_1, \qquad b_4 = \gamma b_1,$$

de sorte que, en posant $\frac{a_1}{b_1} = c$, c étant une quantité que nous déterminerons tout à l'heure, on peut écrire

$$a_1 = c, \qquad a_2 = -i\gamma^3 c, \qquad a_3 = -\gamma^2 c, \qquad a_4 = i\gamma c,$$

$$b_1 = 1, \qquad b_2 = \gamma^3, \qquad b_3 = \gamma^2, \qquad b_4 = \gamma.$$

La relation (4) devient alors

$$(5)\qquad c\,\frac{x_2-i\gamma^3x_1-\gamma^2x_4+i\gamma x_3}{x_2+\gamma^3x_1+\gamma^2x_4+\gamma x_3} = \frac{1}{c}\,\frac{x_1+\gamma^3x_2+\gamma^2x_3+\gamma x_4}{x_1-i\gamma^3x_2-\gamma^2x_3+i\gamma x_4}.$$

Il est facile de voir que cette relation n'est pas une identité; cherchons donc à y satisfaire en tenant compte de (2). Pour cela écrivons (5) de la façon suivante :

$$\begin{aligned} &c^2(x_2-i\gamma^3x_1-\gamma^2x_4+i\gamma x_3)(x_1-i\gamma^3x_2-\gamma^2x_3+i\gamma x_4)\\ -\ &(x_2+\gamma^3x_1+\gamma^2x_4+\gamma x_3)(x_1+\gamma^3x_2+\gamma^3x_3+\gamma x_4) = 0. \end{aligned}$$

En désignant par h, k deux constantes à déterminer, on aura l'identité

$$\begin{aligned} &c^2(x_2-i\gamma^3x_1-\gamma^2x_4+i\gamma x_3)(x_1-i\gamma^3x_2-\gamma^2x_3+i\gamma x_4)\\ -\ &(x_2+\gamma^3x_1+\gamma^2x_4+\gamma x_3)(x_1+\gamma^3x_2+\gamma^2x_3+\gamma x_4)\\ &\qquad + h(x_1+x_2+x_3+x_4)^2 + k(x_1^2+x_2^2+x_3^2+x_4^2) = 0, \end{aligned}$$

et en égalant à zéro les coefficients de tous les termes du premier

membre :

$$-i\gamma^3 c^2 - \gamma^3 + h + k = 0, \qquad (1-\gamma^2)c^2 - (1+\gamma^2) + 2h = 0,$$
$$2i\gamma c^2 - 2\gamma + 2h = 0,$$

d'où

$$c^2 = \frac{1+\gamma^2-2\gamma}{1-\gamma^2-2i\gamma} = \left(\frac{1-\gamma}{1-i\gamma}\right)^2,$$

et, en choisissant arbitrairement le signe de c,

$$c = \frac{1-\gamma}{1-i\gamma}.$$

Nous devons prendre pour γ une racine d'ordre 4 de l'unité, qui ne rende c ni nul, ni infini. Prenons par exemple $\gamma = -1$, on a

$$c = \frac{2}{1+i} = 1-i,$$

d'où

$$a_1 = 1-i, \qquad a_2 = i(1-i), \qquad a_3 = -(1-i), \qquad a_4 = -i(1-i),$$
$$b_1 = 1, \qquad b_2 = -1, \qquad b_3 = 1, \qquad b_4 = -1,$$

de sorte que z a pour expression

$$z = (1-i)\frac{x_1 + ix_2 - x_3 - ix_4}{x_1 - x_2 + x_3 - x_4}.$$

Posons, pour abréger,

$$(6)\quad \begin{cases} p_1 = x_1 + i\,x_2 + i^2 x_3 + i^3 x_4 = x_1 + ix_2 - x_3 - ix_4, \\ p_2 = x_1 + i^2 x_2 + i^4 x_3 + i^6 x_4 = x_1 - x_2 + x_3 - x_4, \\ p_3 = x_1 + i^3 x_2 + i^6 x_3 + i^9 x_4 = x_1 - ix_2 - x_3 + ix_4. \end{cases}$$

Nous aurons

$$(7)\qquad z = (1-i)\frac{p_1}{p_2};$$

de plus la première des relations (2) et la relation (6) donnent

$$(8)\quad \begin{cases} x_1 = \frac{1}{4}\,(p_1 + p_2 + p_3), \\ x_2 = \frac{1}{4}(i^3 p_1 + i^2 p_2 + i\,p_3) = \frac{1}{4}(-ip_1 - p_2 + ip_3), \\ x_3 = \frac{1}{4}(i^6 p_1 + i^4 p_2 + i^2 p_3) = \frac{1}{4}(-p_1 + p_2 - p_3), \\ x_4 = \frac{1}{4}(i^9 p_1 + i^6 p_2 + i^3 p_3) = \frac{1}{4}\,(ip_1 - p_2 - ip_3), \end{cases}$$

équations que nous pouvons résumer dans la suivante :

$$x_{h+1} = \frac{1}{4}(i^{3h}p_1 + i^{2h}p_2 + i^h p_3) \qquad (h = 0, 1, 2, 3).$$

La seconde des équations (2) devient, dans ces conditions,

$$0 = p_1^2 \sum_h i^{6h} + p_2^2 \sum_h i^{4h} + p_3^2 \sum_h i^{2h}$$
$$+ 2p_2p_3 \sum_h i^{3h} + 2p_3p_1 \sum_h i^{4h} + 2p_1p_2 \sum_h i^{5h}.$$

Les propriétés connues des racines de l'unité montrent que les sommes figurant dans le second membre sont nulles, sauf celles dont l'exposant est 4 ou un de ses multiples; ces dernières sommes sont égales à 4. Il reste simplement

$$(9) \qquad p_2^2 + 2p_1p_3 = 0.$$

En se reportant aux égalités (6) on voit que les p_i peuvent être regardés comme les coordonnées homogènes des points du plan de la conique principale; (9) est alors l'équation de cette conique.

Elle passe par les deux sommets (0, 0, 1), (1, 0, 0) du triangle fondamental; z peut être considéré comme le paramètre des rayons correspondants des deux faisceaux passant par ces deux points et dont l'intersection engendre la conique, puisque, d'après (7) et (9), on a

$$(10) \qquad z = (1 - i)\frac{p_1}{p_2} = -\frac{1}{1+i}\frac{p_2}{p_3}.$$

Désignons par $s_1, s_2, \ldots$ les sommes des puissances semblables des racines de (1) et par $c_1, c_2, \ldots$ les sommes des racines, de leurs produits deux à deux, etc. De (2) résulte

$$s_1 = 0, \qquad s_2 = 0,$$

puis, en tenant compte des formules de Newton (*voir* n° 149),

$$s_3 = 3c_3, \qquad s_4 = -4c_4,$$

ou bien

$$s_3 = -12a, \qquad s_4 = -4b.$$

Calculons s_3 et s_4 à l'aide de (8). Nous avons

$$s_3 = \frac{1}{64}\Big(p_1^3\sum_h i^{9h} + p_2^3\sum_h i^{6h} + p_3^3\sum_h i^{3h} + 3p_2^2p_3\sum_h i^{5h}$$
$$+ 3p_2p_3^2\sum_h i^{4h} + 3p_3^2p_1\sum_h i^{5h} + 3p_3p_1^2\sum_h i^{7h}$$
$$+ 3p_1^2p_2\sum_h i^{8h} + 3p_1p_2^2\sum_h i^{7h} + 6p_1p_2p_3\sum_h i^{6h}\Big),$$

qui, à cause des propriétés des racines de l'unité, se réduit à

$$s_3 = \frac{3}{16}p_2(p_1^2 + p_3^2).$$

De même

$$s_4 = \frac{1}{256}\Big(p_1^4\sum_h i^{12h} + p_2^4\sum_h i^{8h} + p_3^4\sum_h i^{4h} + 6p_2^2p_3^2\sum_h i^{6h}$$
$$+ 6p_3^2p_1^2\sum_h i^{8h} + 6p_1^2p_2^2\sum_h i^{10h} + 4p_2^3p_3\sum_h i^{7h}$$
$$+ 4p_2p_3^3\sum_h i^{5h} + 4p_3^3p_1\sum_h i^{6h} + 4p_3p_1^3\sum_h i^{10h}$$
$$+ 4p_1^3p_2\sum_h i^{11h} + 4p_1p_2^3\sum_h i^{9h} + 12p_1^2p_2p_3\sum_h i^{9h}$$
$$+ 12p_2^2p_3p_1\sum_h i^{8h} + 12p_3^2p_1p_2\sum_h i^{7h}\Big)$$

se réduit à

$$s_4 = \frac{1}{64}(p_1^4 + p_2^4 + p_3^4 + 6p_1^2p_3^2 + 12p_1p_2^2p_3)$$

et, en vertu de (9), prend la forme

$$s_4 = \frac{1}{64}(p_1^4 - 14p_1^2p_3^2 + p_3^4).$$

On a donc

$$a = -\frac{p_2(p_1^2 + p_3^2)}{64}, \qquad b = -\frac{p_1^4 - 14p_1^2p_2^2 + p_3^4}{256}.$$

Mais comme d'après (10)

$$p_1 = -ip_3z^2, \qquad p_2 = -(1+i)p_3z,$$

les relations précédentes deviennent

$$(11)\quad \begin{cases} a = -\dfrac{1+i}{64}\, p_3^3\, z(z^4-1) = -\dfrac{1+i}{64}\, p_3^3\, t(z,\, 1), \\[2mm] b = -\dfrac{p_3^4(z^8+14z^4+1)}{256} = -\dfrac{1}{256}\, p_3^4\, \mathrm{W}(z,\, 1). \end{cases}$$

Divisant membre à membre ces deux relations, puis introduisant le résultat ainsi obtenu dans les expressions de p_1 et p_2, on trouve

$$p_1 = 4(1-i)\frac{b}{a}\,\frac{z^3(z^4-1)}{z^8+14z^4+1},$$

$$p_2 = -8i\,\frac{b}{a}\,\frac{z^2(z^4-1)}{z^8+14z^4+1},$$

$$p_3 = 4(1+i)\frac{b}{a}\,\frac{z(z^4-1)}{z^8+14z^4+1}.$$

Remplaçant enfin dans (8) p_1, p_2, p_3 par ces valeurs, on obtient x_1, x_2, x_3, x_4 exprimés à l'aide de z

$$(12)\quad \begin{cases} x_1 = [\ \ (1-i)z^2 - 2iz + (1+i)]\dfrac{b}{a}\,\dfrac{z(z^4-1)}{z^8+14z^4+1}, \\[2mm] x_2 = [-(1+i)z^2 + 2iz - (1-i)]\dfrac{b}{a}\,\dfrac{z(z^4-1)}{z^8+14z^4+1}, \\[2mm] x_3 = [-(1-i)z^2 - 2iz - (1+i)]\dfrac{b}{a}\,\dfrac{z(z^4-1)}{z^8+14z^4+1}, \\[2mm] x_4 = [\ \ (1+i)z^3 + 2iz + (1-i)]\dfrac{b}{a}\,\dfrac{z(z^4-1)}{z^8+14z^4+1}. \end{cases}$$

z est une racine de l'équation octaédrique

$$\frac{\mathrm{W}^3(z,\, 1)}{108\, t^4(z,\, 1)} = \mathrm{Z},$$

qui, à cause de (11), s'écrit

$$\frac{\mathrm{W}^3(z.\, 1)}{108\, t^4(z,\, 1)} = \frac{b^3}{27a^3}.$$

Cette équation une fois résolue (nº 147), les formules (12) nous donneront les racines de (1).

155. Expliquons maintenant comment on passe de l'équation générale du quatrième degré à une équation ne renfermant ni deuxième, ni troisième terme.

Nous pouvons supposer l'équation, déjà privée de second terme et mise sous la forme

$$(1) \qquad y^4 + 6ay^2 + 4by + c = 0.$$

Soient y_1, y_2, y_3, y_4 les racines de (1); $s_1, s_2, \ldots$ les sommes de leurs puissances semblables.

Posons

$$(2) \qquad x = y^2 + ky - \frac{s_2}{4},$$

k étant une constante quelconque.

L'élimination de y entre (1) et (2) conduit à une équation du quatrième degré en x, ayant pour racines

$$(3) \qquad x_h = y_h^2 + ky_h - \frac{s_2}{4} \qquad (h = 1, 2, 3, 4).$$

Puisque $s_1 = 0$, il résulte de (3)

$$\sum_{h=1}^{4} x_h = s_2 + ks_1 - s_2 = 0.$$

De plus

$$\sum_{h=1}^{4} x_h^2 = s_4 + k^2 s_2 + \frac{s_2^2}{4} + 2ks_3 - \frac{s_2^2}{2} - \frac{ks_1 s_2}{2} = s_2 k^2 + 2s_3 k + s_4 - \frac{s_2^2}{4}.$$

Si donc on veut que l'équation en x soit privée non seulement du second terme, mais encore du troisième, k doit être choisi de façon à satisfaire à l'équation

$$(4) \qquad s_2 k^2 + 2s_3 k + s_4 - \frac{s_2^2}{4} = 0.$$

Mais

$$c_2 = 6a, \qquad c_3 = -4b, \qquad c_4 = c,$$

et, en vertu des formules de Newton,

$$s_2 = -2c_2 = -12a, \qquad s_3 = 3c_3 = -12b,$$
$$s_4 = -4c_4 + 2c_2^2 = -4c + 72a^2.$$

Donc l'équation (4) peut s'écrire

$$k^2 + 2\frac{b}{a}k - \left(3a - \frac{c}{3a}\right) = 0,$$

d'où

$$k = \frac{1}{a}\left(-b \pm \sqrt{b^2 - \frac{ac}{3} + 3a^3}\right).$$

La formule (2) devient alors, en remplaçant k par l'expression précédente,

$$x = y^2 + \frac{1}{a}\left(-b \pm \sqrt{b^2 - \frac{ac}{3} + 3a^3}\right) y + 3a,$$

et l'on a, pour les racines de l'équation transformée,

$$x_h = y_h^2 + \frac{1}{a}\left(-b \pm \sqrt{b^2 - \frac{ac}{3} + 3a^3}\right) y_h + 3a \qquad (h = 1, 2, 3, 4).$$

A l'aide de cette expression et des formules de Newton [1], on peut calculer

$$\sum_{h=1}^{4} x_h^3, \qquad \sum_{h=1}^{4} x_h^4$$

et de là les coefficients de l'équation transformée.

Cette dernière équation une fois résolue, c'est-à-dire une fois x déterminé, l'Algèbre nous apprend à déduire des relations (1) et (2) la valeur de y par des opérations rationnelles.

156. Pour les équations du cinquième degré partons de la forme *principale* [2]

(1) $$x^5 + 5ax^2 + 5bx + c = 0.$$

Soient x_1, x_2, x_3, x_4, x_5 les racines; elles satisfont aux deux

---

[1] Ces formules donnent dans le cas actuel

$$s_5 = 120ab,$$
$$s_6 = 36ac + 48b^2 - 432a^3,$$
$$s_7 = 28bc - 1008a^2b,$$
$$s_8 = 4c^2 - 288a^2c - 768ab^2 + 2592a^4.$$

[2] Nous verrons plus loin comment on peut ramener l'équation générale du cinquième degré à la forme (1).

relations

$$(2) \qquad \sum_{h=1}^{5} x_h = 0,$$

$$(3) \qquad \sum_{h=1}^{5} x_h^2 = 0.$$

Nous pouvons représenter chaque point de l'espace à l'aide de cinq coordonnées homogènes x_h, liées entre elles par la relation (2); de telles coordonnées sont dites *pentaédrales* [1]. A chaque équation (1) correspondront 120 points, puisque, pour représenter les cinq racines, il y a 120 permutations possibles, et ces points sont situés sur la quadrique représentée par l'équation (3) et que nous appellerons *quadrique principale*. Chaque permutation des racines est équivalente à une collinéation, qui transforme la quadrique en elle-même.

Ainsi la permutation $x_{\alpha_1} x_{\alpha_2} x_{\alpha_3} x_{\alpha_4} x_{\alpha_5}$, où les α_h sont à l'ordre près les nombres 1, 2, 3, 4, 5, équivaut à la collinéation

$$(4) \quad x'_1 = x_{\alpha_1}, \qquad x'_2 = x_{\alpha_2}, \qquad x'_3 = x_{\alpha_3}, \qquad x'_4 = x_{\alpha_4}, \qquad x'_5 = x_{\alpha_5}.$$

Voyons comment se comportent les génératrices rectilignes de la surface. Tout d'abord une substitution linéaire changeant une droite en une autre droite, chaque génératrice se transforme en une autre génératrice. Ensuite deux génératrices g_1, g_2, appartenant à un même système, se transforment en deux autres génératrices g'_1, g'_2, appartenant aussi à un même système, car autrement g'_1, g'_2 seraient concourantes, tandis que g_1 et g_2 ne le sont pas. Enfin à deux génératrices de systèmes différents correspondent deux autres génératrices de systèmes différents. Il ne peut donc exister que deux espèces de collinéations : celles qui conservent chaque système de génératrices et celles qui échangent entre eux les deux systèmes. Or, s'il existe une collinéation de la seconde espèce, il en existe nécessairement 60. En effet, soient C_1, C_2, …, C_r les collinéations de la première espèce et D_1, D_2, …, D_s

(1) Nous pouvons prendre pour coordonnées pentaédrales, par exemple, les quatre coordonnées homogènes relatives à un tétraèdre fondamental quelconque et leur somme changée de signe.

celles de la seconde espèce ; on a

$$r + s = 120.$$

Les produits $C_1 D_1$, $C_2 D_1$, ..., $C_r D_1$ constituent r collinéations de seconde espèce toutes distinctes, de sorte que $s \geqq r$; de même les produits $D_1 D_1$, $D_2 D_1$, ..., $D_s D_1$ seront s collinéations distinctes de première espèce, de sorte que $r \geqq s$. Par suite

$$r = s = 60.$$

Il n'y a donc que deux cas possibles : ou bien les 120 collinéations laissent invariable chaque système, ou bien 60 seulement possèdent cette propriété. Dans ce dernier cas, les 60 collinéations correspondent nécessairement aux 60 permutations paires des cinq coordonnées ; elles forment donc (n° 67) un groupe holoédriquement isomorphe au groupe icosaédrique.

Pour distinguer ces deux cas, rappelons que l'équation d'une quadrique peut, par une substitution linéaire convenable, être ramenée à la forme

$$p_1 p_4 + p_2 p_3 = 0,$$

où les p_h sont des coordonnées tétraédrales. On peut écrire

$$\frac{p_1}{p_2} = -\frac{p_3}{p_4} = \lambda, \qquad \frac{p_1}{p_3} = -\frac{p_2}{p_4} = \mu,$$

λ, μ sont alors les paramètres des génératrices des deux systèmes. Ce sont des fonctions linéaires des cordonnées p_h et, par suite, des coordonnées x_h. Donc, à toute transformation linéaire des coordonnées x_h qui conserve chacun des deux systèmes de génératrices correspondra tant pour λ que pour μ une substitution linéaire. Nous obtenons ainsi un groupe G de substitutions linéaires de λ, holoédriquement isomorphe au groupe des collinéations, conservant chacun des deux systèmes de génératrices.

Par conséquent le groupe G est, ou bien de soixantième ordre, et c'est alors un groupe icosaédrique, ou bien il est du cent-vingtième ordre et il contient alors un sous-groupe icosaédrique. Mais ce dernier cas est impossible, car (n° 37) les groupes de substitutions linéaires du cent-vingtième ordre étant des groupes cycliques ou diédriques ne peuvent contenir aucun sous-groupe icosaédrique. Nous arrivons donc à la conclusion suivante :

Des 120 *collinéations* (4), 60 *seulement conservent chaque système de génératrices; les substitutions correspondantes du paramètre des génératrices de l'un ou de l'autre système forment un groupe icosaédrique.*

Nous avons déjà établi dans tous ses détails l'isomorphisme du groupe des 60 permutations paires de 5 éléments et du groupe icosaédrique (n° 67); et nous avons vu qu'aux substitutions S, T de ce groupe correspondent respectivement les permutations (23451), (13254).

Cherchons donc à construire une fonction linéaire z des x_h, qui subisse les substitutions S, T quand on effectue sur les x les deux permutations précédentes.

Posons

$$z = \frac{a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + a_5 x_5}{b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 + b_5 x_5}.$$

Les substitutions S, T ont respectivement pour expressions

$$z' = \varepsilon z, \qquad z' = \frac{\sigma z + \tau}{\tau z - \sigma},$$

où ε, σ, τ ont la même signification qu'au n° 68.

On doit avoir

$$(5)\quad \left\{\begin{aligned} &\frac{a_1 x_2 + a_2 x_3 + a_3 x_4 + a_4 x_5 + a_5 x_1}{b_1 x_2 + b_2 x_3 + b_3 x_4 + b_4 x_5 + b_5 x_1} \\ &\qquad = \varepsilon \frac{a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + a_5 x_5}{b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 + b_5 x_5}, \\ &\frac{a_1 x_1 + a_2 x_3 + a_3 x_2 + a_4 x_5 + a_5 x_4}{b_1 x_1 + b_2 x_3 + b_3 x_2 + b_4 x_5 + b_5 x_4} \\ &\qquad = \frac{(\sigma a_1 + \tau b_1) x_1 + \ldots + (\sigma a_5 + \tau b_5) x_5}{(\tau a_1 - \sigma b_1) x_1 + \ldots + (\tau a_5 - \sigma b_5) x_5}. \end{aligned}\right.$$

Pour que la première équation (5) soit satisfaite indépendamment des relations (2), (3), qui lient les x_h, on doit avoir

$$\frac{a_5}{\varepsilon a_1} = \frac{a_1}{\varepsilon a_2} = \frac{a_2}{\varepsilon a_3} = \frac{a_3}{\varepsilon a_4} = \frac{a_4}{\varepsilon a_5} = \frac{b_5}{b_1} = \frac{b_1}{b_2} = \frac{b_2}{b_3} = \frac{b_3}{b_4} = \frac{b_4}{b_5},$$

ou, en désignant par δ la valeur commune de ces rapports,

$$\delta^5 = 1,$$

$$\begin{aligned} &a_2 = \varepsilon^4 \delta^4 a_1, && a_3 = \varepsilon^3 \delta^3 a_1, && a_4 = \varepsilon^2 \delta^2 a_1, && a_5 = \varepsilon \delta a_1, \\ &b_2 = \delta^4 b_1, && b_3 = \delta^3 b_1, && b_4 = \delta^2 b_1, && b_5 = \delta b_1. \end{aligned}$$

Soit $\frac{a_1}{b_1} = c$, c étant une quantité qu'on déterminera plus loin ; on peut écrire

$$\begin{array}{lllll} a_1 = c, & a_2 = \varepsilon^4 \delta^4 c, & a_3 = \varepsilon^3 \delta^3 c, & a_4 = \varepsilon^2 \delta^2 c, & a_5 = \varepsilon \delta c, \\ b_1 = 1, & b_2 = \delta^4, & b_3 = \delta^3, & b_4 = \delta^2, & b_5 = \delta \end{array}$$

et l'expression de z devient

$$z = c \frac{x_1 + \varepsilon^4 \delta^4 x_2 + \varepsilon^3 \delta^3 x_3 + \varepsilon^2 \delta^2 x_4 + \varepsilon \delta x_5}{x_1 + \varepsilon^{h+1} x_2 + \varepsilon^{2(h+1)} x_3 + \varepsilon^{3(h+1)} x_4 + \varepsilon^{4(h+1)} x_5}.$$

Il est clair que z satisfait à la condition cherchée, quel que soit h. Posons

(6) $$p_h = x_1 + \varepsilon^h x_2 + \varepsilon^{2h} x_3 + \varepsilon^{3h} x_4 + \varepsilon^{4h} x_5 \qquad (h = 1, 2, 3, 4),$$

d'où

(7) $$z = c \frac{p_h}{p_{h+1}}.$$

Les p_h peuvent être considérés comme coordonnées homogènes des points de l'espace ; les expressions de x_h à l'aide des p_h s'obtiennent au moyen des relations (2) et (6) ; on trouve ainsi :

$$\begin{aligned} x_1 &= \frac{1}{5}(p_1 + p_2 + p_3 + p_4), \\ x_2 &= \frac{1}{5}(\varepsilon^4 p_1 + \varepsilon^8 p_2 + \varepsilon^{12} p_3 + \varepsilon^{16} p_4), \\ x_3 &= \frac{1}{5}(\varepsilon^3 p_1 + \varepsilon^6 p_2 + \varepsilon^9 p_3 + \varepsilon^{12} p_4), \\ x_4 &= \frac{1}{5}(\varepsilon^2 p_1 + \varepsilon^4 p_2 + \varepsilon^6 p_3 + \varepsilon^8 p_4), \\ x_5 &= \frac{1}{5}(\varepsilon p_1 + \varepsilon^2 p_2 + \varepsilon^3 p_3 + \varepsilon^4 p_4), \end{aligned}$$

et (3) devient

$$p_1 p_4 + p_2 p_3 = 0,$$

de sorte que, en faisant dans (7) $h = 1$, nous avons

(8) $$z = c \frac{p_1}{p_2} = - c \frac{p_2}{p_3}$$

et z peut être considéré comme le paramètre des génératrices rectilignes d'un des deux systèmes.

Reste à déterminer c, de façon que la seconde équation (5) soit satisfaite. Remplaçons dans cette équation z par l'expression (8); on obtient, en vertu des relations (2) et (3),

$$\begin{aligned}
& c(x_1+\varepsilon^2 x_2+\varepsilon x_3+\varepsilon^4 x_4+\varepsilon^3 x_5) \\
&\quad \times [(c\tau-\sigma)x_1+(c\varepsilon\tau-\varepsilon^2\sigma)x_2+(c\varepsilon^2\tau-\varepsilon^4\sigma)x_3 \\
&\qquad\qquad +(c\varepsilon^3\tau-\varepsilon^6\sigma)x_4+(c\varepsilon^4\tau-\varepsilon^8\sigma)x_5] \\
&\quad -(x_1+\varepsilon^4 x_2+\varepsilon^2 x_3+\varepsilon^8 x_4+\varepsilon^6 x_5) \\
&\quad \times [(c\sigma+\tau)x_1+(c\varepsilon\sigma+\varepsilon^2\tau)x_2+(c\varepsilon^2\sigma+\varepsilon^4\tau)x_3 \\
&\qquad\qquad +(c\varepsilon^3\sigma+\varepsilon^6\tau)x_4+(c\varepsilon^4\sigma+\varepsilon^8\tau)x_5] \\
&\quad + h(x_1+x_2+x_3+x_4+x_5)^2+k(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2)=0
\end{aligned}$$

(h, k sont des constantes à déterminer); ou bien, sous une forme plus concise,

$$\sum_{ij} a_{ij}x_i x_j = 0,$$

les coefficients a_{ij} ayant pour expressions

$$\begin{aligned}
a_{11} &= c^2\tau-2c\sigma-\tau+h+k, \\
a_{22} = a_{33} &= c^2\varepsilon^3\tau-c(1+\varepsilon^4)\sigma-\varepsilon\tau+h+k, \\
a_{44} = a_{55} &= c^2\varepsilon^2\tau-c(1+\varepsilon)\sigma-\varepsilon^4\tau+h+k, \\
a_{12} = a_{13} &= c^2(\varepsilon+\varepsilon^2)\tau-c(\varepsilon+2\varepsilon^2+\varepsilon^4)\sigma-(\varepsilon+\varepsilon^4)\tau+2h, \\
a_{14} = a_{15} &= c^2(\varepsilon^3+\varepsilon^4)\tau-c(\varepsilon+2\varepsilon^3+\varepsilon^4)\sigma-(\varepsilon+\varepsilon^3)\tau+2h, \\
a_{23} &= c^2(\varepsilon^2+\varepsilon^4)\tau-2c(\varepsilon+\varepsilon^3)\sigma-(\varepsilon^3+\varepsilon^4)\tau+2h, \\
a_{24} = a_{35} &= 2c^2\tau+c\sigma-2\tau+2h, \\
a_{25} = a_{34} &= c^2(\varepsilon+\varepsilon^4)\tau-c(2+\varepsilon^2+\varepsilon^3)\sigma-(\varepsilon^2+\varepsilon^3)\tau+2h, \\
a_{45} &= c^2(\varepsilon+\varepsilon^3)\tau-2c(\varepsilon^2+\varepsilon^4)\sigma-(\varepsilon+\varepsilon^2)\tau+2h.
\end{aligned}$$

Ces coefficients doivent être tous nuls. On aura donc, en tenant compte des expressions de σ et τ,

$$\begin{aligned}
0 = a_{44}-a_{22} &= c^2(\varepsilon^2-\varepsilon^3)\tau-c(\varepsilon-\varepsilon^4)\sigma+(\varepsilon-\varepsilon^4)\tau = c^2\tau^2-c\sigma^2+\sigma\tau, \\
0 = a_{45}-a_{23} &= c^2(\varepsilon-\varepsilon^4-\varepsilon^2+\varepsilon^3)\tau \\
&\quad -2c(\varepsilon^2-\varepsilon^3-\varepsilon+\varepsilon^4)\sigma-(\varepsilon-\varepsilon^4+\varepsilon^2-\varepsilon^3)\tau \\
&= c^2(\sigma-\tau)\tau-2c(\tau-\sigma)\sigma-(\sigma+\tau)\tau.
\end{aligned}$$

Éliminant c^2 entre ces deux équations, il vient

$$c = \frac{\tau(\sigma^2+\tau^2)}{\sigma^3+\sigma^2\tau-2\sigma\tau^2}.$$

Or, puisque (n° 68)

$$\sigma^2-\tau^2 = \sigma\tau,$$

on a

$$\sigma^3 + \sigma^2\tau - 2\sigma\tau^2 = \sigma(\sigma\tau + \tau^2) + \sigma^2\tau - 2\sigma\tau^2 = \tau(2\sigma^2 - \sigma\tau) = \tau(\sigma^2 + \tau^2);$$

par suite $c = 1$, et il est facile de vérifier que cette valeur de c satisfait à toutes les équations obtenues en éliminant h et k entre les $a_{ij} = 0$.

L'expression cherchée de z est, d'après cela,

$$z = \frac{p_1}{p_2} = -\frac{p_3}{p_4}.$$

Nous allons démontrer que, si l'équation donnée est la résolvante principale d'une équation icosaédrique, la fonction z construite précédemment n'est autre que la variable z qui figure dans cette équation icosaédrique.

Les racines de la résolvante principale sont (nº 149)

$$Y_h = aW_h + bt_hW_h \qquad (h = 0, 1, 2, 3, 4).$$

Or, on peut écrire

$$W_h = (\varepsilon^{4h}z_1 + \varepsilon^{3h}z_2)(-z_1^7 - 7z_1^2z_2^5) + (\varepsilon^{2h}z_1 - \varepsilon^h z_2)(-7z_1^5z_2^2 + z_2^7),$$
$$t_hW_h = (\varepsilon^{4h}z_1 + \varepsilon^{3h}z_2)(26z_1^{10}z_2^3 + 39z_1^5z_2^8 - z_2^{13})$$
$$+ (\varepsilon^{2h}z_1 - \varepsilon^h z_2)(-z_1^{13} - 39z_1^8z_2^5 + 26z_1^3z_2^{10}).$$

Posant ensuite

$$a(-z_1^7 - 7z_1^2z_2^5) + b(26z_1^{10}z_2^3 + 39z_1^5z_2^8 - z_2^{13}) = R,$$
$$a(-7z_1^5z_2^2 + z_2^7) + b(-z_1^{13} - 39z_1^8z_2^5 + 26z_1^3z_2^{10}) = S,$$

expressions qui sont indépendantes de l'indice h, on obtient

$$Y_h = R(\varepsilon^{4h}z_1 + \varepsilon^{3h}z_2) + S(\varepsilon^{2h}z_1 - \varepsilon^h z_2).$$

Il suit de là

$$p_1 = Y_0 + \varepsilon Y_1 + \varepsilon^2 Y_2 + \varepsilon^3 Y_3 + \varepsilon^4 Y_4$$
$$= \sum_{h=0}^{4} [R(z_1 + \varepsilon^{4h}z_2) + S(\varepsilon^{3h}z_1 - \varepsilon^{2h}z_2)] = 5Rz_1,$$
$$p_2 = Y_0 + \varepsilon^2 Y_1 + \varepsilon^4 Y_2 + c^6 Y_3 + \varepsilon^8 Y_4$$
$$= \sum_{h=0}^{4} [R(\varepsilon^h z_1 + z_2) + S(\varepsilon^{4h}z_1 - \varepsilon^{3h}z_2)] = 5Rz_2,$$

$$p_3 = Y_0 + \varepsilon^3 Y_1 + \varepsilon^6 Y_2 + \varepsilon^9 Y_3 + \varepsilon^{12} Y_4$$
$$= \sum_{h=0}^{4} [R(\varepsilon^{2h} z_1 + \varepsilon^h z_2) + S(z_1 - \varepsilon^{4h} z_2)] = 5 S z_1,$$
$$p_4 = Y_0 + \varepsilon^4 Y_1 + \varepsilon^8 Y_2 + \varepsilon^{12} Y_3 + \varepsilon^{16} Y_4$$
$$= \sum_{h=0}^{4} [R(\varepsilon^{3h} z_1 + \varepsilon^{2h} z_2) + S(\varepsilon^h z_1 - z_2)] = -5 S z_2,$$

d'où

$$\frac{p_1}{p_2} = \frac{z_1}{z_2}, \qquad \frac{p_3}{p_4} = -\frac{z_1}{z_2}$$

ou bien

$$z = \frac{p_1}{p_2} = -\frac{p_3}{p_4}.$$

Ainsi, étant donnée une équation principale du cinquième degré, s'il est possible de former l'équation icosaédrique dont elle est la résolvante principale, la résolution de cette dernière équation nous fera connaître immédiatement les racines de l'équation donnée. Cela tient à ce que, la résolvante principale de l'équation icosaédrique étant (comme d'ailleurs toutes ses résolvantes) une résolvante équivalente, l'équation icosaédrique peut à son tour être regardée comme résolvante de sa propre résolvante.

Soit donc l'équation

$$x^5 + 5ax^2 + 5bx + c = 0.$$

Si nous pouvons déterminer trois quantités m, n, Z de façon à identifier cette équation avec (n° 149)

$$x^5 - \frac{5}{Z}\left(8m^3 + 12m^2n + \frac{6mn^2 + n^3}{1 - Z}\right)x^2$$
$$+ \frac{15}{Z}\left[-4m^4 + \frac{6m^2n^2 + 4mn^3}{1 - Z} + \frac{3}{4}\,\frac{n^4}{(1 - Z)^2}\right]x$$
$$- \frac{3}{Z}\left[48m^5 - \frac{40m^3n^3}{1 - Z} + \frac{15mn^4 + 4n^2}{(1 - Z)^2}\right] = 0,$$

et si z est une racine de l'équation icosaédrique

$$-\frac{H^3(z, 1)}{1728 f^5(z, 1)} = Z,$$

les expressions

$$x_h = m v_h(z) + n u_h(z) v_h(z) \qquad (h = 0, 1, 2, 3, 4),$$

où

$$u_h(z) = \frac{12 f^2(z, 1)}{T(z, 1)} t_h(z, 1), \qquad v_h(z) = \frac{12 f(z, 1)}{H(z, 1)} W_h(z, 1),$$

donneront les cinq racines de l'équation proposée.

On est donc amené à résoudre par rapport à m, n, Z le système d'équations

$$(1) \qquad a = -\frac{1}{Z}\left(8m^3 + 12m^2 n + \frac{6mn^2 + n^3}{1 - Z}\right),$$

$$(2) \qquad b = \frac{3}{Z}\left[-4m^4 + \frac{6m^2n^2 + 4mn^3}{1 - Z} + \frac{3}{4}\frac{n^4}{(1 - Z)^2}\right],$$

$$(3) \qquad c = -\frac{3}{Z}\left[48m^5 - \frac{40m^3n^2}{1 - Z} + \frac{15mn^4 + 4n^5}{(1 - z)^2}\right].$$

On déduit de (1), (2) et (3)

$$\frac{12n^2}{1 - Z} a + 12mb - c = 0$$

ou bien

$$(4) \qquad \frac{n^2}{1 - Z} = \frac{-12mb + c}{12a}.$$

De plus

$$(5) \qquad \begin{cases} \dfrac{n^2}{1 - Z} b + mc = \dfrac{9}{4Z}\left[-64m^6 + \dfrac{48m^4n^2}{1 - Z} - \dfrac{12m^2n^4}{(1 - Z)^2} + \dfrac{n^6}{(1 - Z)^3}\right] \\ \qquad = -\dfrac{9}{4Z}\left(4m^2 - \dfrac{n^2}{1 - Z}\right)^3, \end{cases}$$

$$(6) \qquad -3ma + 2b = \frac{9n}{2Z}\left[8m^3 + \frac{12m^2n + 6mn^2}{1 - Z} + \frac{n^3}{(1 - Z)^2}\right].$$

Les relations (1) et (6) donnent ensuite

$$a^2 - \frac{4}{81}\frac{1 - Z}{n^2}(-3ma + 2b)^2$$
$$= \frac{1}{Z}\left[64m^6 - \frac{48m^4n^2}{1 - Z} + \frac{12m^2n^4}{(1 - Z)^2} - \frac{n^6}{(1 - Z)^3}\right] = \frac{1}{Z}\left(4m^2 - \frac{n^2}{1 - Z}\right)^3$$

et en comparant avec (5) on obtient

$$\frac{n^2}{1 - Z} b + mc = -\frac{9}{4}\left[a^2 - \frac{4}{81}\frac{1 - Z}{n^2}(-3ma + 2b)^2\right]$$

ou bien, multipliant par $\frac{n^2}{1-z}$ et faisant passer tous les termes dans le premier membre,

$$\frac{n^2}{1-Z}\left(\frac{9}{4}a^2+\frac{n^2}{1-Z}b+mc\right)-\frac{1}{9}(-3ma+2b)^2=0.$$

et enfin, en tenant compte de (4),

$$\frac{-12mb+c}{12a}\left[\frac{9}{4}a^2+\frac{(-12mb+c)b}{12a}+mc\right]-\frac{1}{9}(-3ma+2b)^2=0.$$

Cette équation renferme une seule inconnue m; elle est du second degré. En l'ordonnant, il vient

$$\begin{aligned}&144(b^3-a^4-abc)m^2\\&\quad-12(2b^2c+11a^3b-ac^2)m+bc^2+27a^3c-64a^2b^2=0,\end{aligned}$$

d'où

(7) $$m=\frac{2b^2c+11a^3b-ac^2\pm a\Delta}{24(b^3-a^4-abc)},$$

Δ^2 ayant pour valeur

$$108a^5c-135a^4b^2+90a^2bc^2-320ab^3c+256b^5+c^4.$$

L'expression Δ^2 est, au facteur 5 près, le discriminant de l'équation donnée (*voir* nº **149**).

Les relations (4) et (5) donnent ensuite

$$\frac{(-2mb+c)b}{12a}+mc=-\frac{9}{4Z}\left(4m^2+\frac{12mb-c}{12a}\right)^3,$$

d'où

(8) $$Z=-\frac{(48am^2+12bm-c)^3}{64a^2[-12(b^2-ac)m+bc]},$$

où m doit être remplacée par son expression (7).

Enfin, de (1) et (4) on déduit

$$\begin{aligned}-aZ&=8m^3+12m^2n+\frac{n^2}{1-Z}(6m+n)\\&=8m^3+12m^2n+\frac{(6m+n)(-12bm+c)}{12a}\end{aligned}$$

et, en résolvant par rapport à n,

(9) $$n=\frac{-96am^3+72bm^2-6cm-12a^2Z}{144am^2-12bm+c},$$

où, bien entendu, on a remplacé m et Z par leurs expressions (7) et (8).

Les relations (7), (8), (9) résolvent le problème proposé.

Le double signe ($\pm$) provient de ce que la quadrique principale admet deux systèmes de génératrices rectilignes.

157. Pour terminer, voyons comment une équation quelconque du cinquième degré peut se ramener à une équation principale.

Soient y_1, y_2, y_3, y_4, y_5 les racines de l'équation donnée, que nous supposerons privée de second terme, en sorte que $s_1, s_2, \ldots$ étant les sommes des puissances semblables des y, on a $s_1 = 0$. Posons

$$y_{kh} = y_h^k - \frac{s_k}{5} \qquad (h = 1, 2, 3, 4, 5;\ k = 1, 2, 3, 4);$$

on aura

$$(1) \qquad \sum_{h=1}^{5} y_{kh} = 0 \qquad (k = 1, 2, 3, 4).$$

Donc les systèmes de valeurs

$$y_{k1},\quad y_{k2},\quad y_{k3},\quad y_{k4},\quad y_{k5} \qquad (k = 1, 2, 3, 4)$$

peuvent être regardés comme les coordonnées pentaédrales de quatre points de l'espace. Prenons ces quatre points comme sommets du tétraèdre fondamental, et soient p, q, r, s les coordonnées tétraédrales d'un point quelconque de l'espace. Les coordonnées pentaédrales du même point sont

$$(2) \qquad x_h = p y_{1h} + q y_{2h} + r y_{3h} + s y_{4h} \qquad (h = 1, 2, 3, 4, 5)$$

et, d'après (1), elles vérifient l'équation fondamentale

$$\sum_{h=1}^{5} x_h = 0;$$

si nous parvenons à déterminer p, q, r, s de façon qu'elles vérifient en même temps

$$(3) \qquad \sum_{h=1}^{5} x_h^2 = 0,$$

la transformation

$$(4) \qquad x = py + q\left(y^2 - \frac{s_2}{5}\right) + r\left(y^3 - \frac{s_3}{5}\right) + s\left(y^4 - \frac{s_4}{5}\right)$$

ramènera l'équation donnée à une équation principale.

La détermination de p, q, r, s, dans les conditions indiquées, peut se faire d'une infinité de manières. Remplaçons en effet dans (3) les x_h par leurs expressions (2), nous obtenons l'équation du second degré

$$(5) \qquad p^2 \sum_{h=1}^{5} y_{1h}^2 + q^2 \sum_{h=1}^{5} y_{2h}^2 + \ldots + 2pq \sum_{h=1}^{5} y_{1h} y_{2h} + \ldots = 0,$$

homogène en p, q, r, s et dont les coefficients sont des fonctions rationnelles des coefficients de l'équation proposée; si l'on se donne arbitrairement les valeurs de trois des quantités p, q, r, s, la quatrième est déterminée par une équation du second degré.

Au point de vue géométrique l'équation (5) représente la quadrique principale, et notre problème revient à la détermination d'un quelconque de ses points.

On peut procéder ainsi : choisissons deux points quelconques de l'espace (p_1, q_1, r_1, s_1), (p_2, q_2, r_2, s_2); tout point de la droite passant par ces deux points aura pour coordonnées

$$(6) \qquad \begin{cases} p = \rho_1 p_1 + \rho_2 p_2, & q = \rho_1 q_1 + \rho_2 q_2, \\ r = \rho_1 r_1 + \rho_2 r_2, & s = \rho_1 s_1 + \rho_2 s_2, \end{cases}$$

ρ_1, ρ_2 étant des coefficients indéterminés. Introduisons ces expressions dans l'équation (5), elle se transforme en une équation du second degré par rapport à $\frac{\rho_1}{\rho_2}$.

Si nous remplaçons, dans l'équation (5), ρ_1 et ρ_2 par les valeurs correspondant à l'une ou l'autre de ces deux racines, nous obtenons un système de valeurs de p, q, r, s qui satisfont à la condition cherchée.

L'équation principale une fois résolue, les cinq valeurs de x sont déterminées et la théorie de l'élimination permet de trouver rationnellement, à l'aide des équations (1) et (4), les cinq valeurs correspondantes de y.

FIN.

NIDEX ALPHABÉTIQUE.

ERRATA.

Page 1, ligne 8 du texte, supprimer les mots *unique* et lire « *un* élément d'une certaine classe à *un* autre élément de la même classe ».

Page 60, ligne 10, *au lieu de* groupe rectangulaire, *lire* groupe trirectangle.

TABLE DES MATIÈRES.

PARIS. — IMPRIMERIE GAUTHIER-VILLARS,

44087 Quai des Grands-Augustins, 55.

BINDING SECT. JUN 14 1982

PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET

UNIVERSITY OF TORONTO LIBRARY

QA Vivanti, Guilio
343 Les fonctions polyédriques
V513

94